Framtidens Brott

Den Kriminella Spelplanen – mitt i vår vardag

Ett initiativ av SSF

Utgåva 1, dec 2024

Konceptet Framtidens Brott är en serie av publikationer som utforskar framtidens brottslighet ur olika perspektiv.

UTGÅVA 1

Ger en nulägesanalys av den *kriminella spelplanen* och vart den kan vara på väg.
Lanseras kvartal 4 2024.

UTGÅVA 2

Fokuserar på nya former av brottslighet.
Lanseras kvartal 2 2025.

UTGÅVA 3

Samproduceras tillsammans med partners. Tema sätts längre fram.
Planerad lansering kvartal 3 2025.

UTGÅVA 4

Samproduceras tillsammans med partners. Tema sätts längre fram.
Planerad lansering kvartal 4 2025.

Innehåll

Sammanfattning

Kriminaliteten har de senaste åren blivit både global och mer komplex. Nya teknologier och digitala plattformar har gett kriminella grupper möjligheter att växa, organisera sig och verka över nationsgränser.

Vi på SSF, som ägnar oss helhjärtat åt brottsförebyggande arbete, är intresserade av att ta reda på mer om den internationella kriminella marknadens dynamik – från drogförsäljning och smuggling till mäktiga brottssyndikat och avancerade cybergrupper som attackerar företag, institutioner och privatpersoner för pengar eller politiska syften. För att få en bättre överblick tog vi därför fram "Den Kriminella Spelplanen", en karta som hjälper oss att bättre förstå det kriminella landskapet i vår vardag. Nu delar vi denna rapport med dig, i hopp om att den kan stödja och inspirera även i ditt arbete.

Vi har kartlagt hur kriminella nätverk organiserar sig, utvecklas och verkar över nationsgränser, samt vilka konsekvenser detta får för företag, samhälle och enskilda individer. Genom att studera marknadsstrukturer, nyckelaktörer och den ekonomiska logik som driver utvecklingen belyser rapporten inte bara rådande mönster, utan även framväxande trender och tänkbara framtida utmaningar. Insikterna har vi inhämtat från ett stort urval av rapporter, artiklar, böcker, forskning och genom intervjuer med experter med stor förståelse av den kriminella spelplanen.

Analysen visar att kriminella nätverk, från hierarkiskt organiserade brottssyndikat till löst sammansatta digitala grupperingar drar nytta av globalisering och teknisk utveckling. Genom att infiltrera den legala ekonomin och utnyttja svårigheterna att genomdriva internationella lagar, får de tillgång till nya illegala marknader, bland annat inom välfärdsbrott och penningtvätt. Detta påverkar inte bara lokala ekonomier och försämrar företagsklimatet, utan undergräver även förtroendet för samhällsinstitutioner och politiska system.

Kriminell verksamhet inverkar på människors vardag på flera plan. Narkotikahandel, hot och våld i bostadsområden och offentliga miljöer skapar otrygghet. Välfärdsbrott och digitala angrepp som bedrägerier, identitetsstölder och dataintrång bidrar till oro och kräver ökad vaksamhet. Företag utsätts för hot och utpressning och tyngs av stigande säkerhetskostnader.

Digitalisering, ny teknik och omfattande datainsamling skapar nya möjligheter för bedrägerier. Hyperpersonlig data, som det samlas in alltmer av, kan bli ett ännu större mål för kriminella under de kommande åren.

Den kriminella ekonomin är omfattande, och inte minst den illegala narkotikahandeln präglas av hård konkurrens. Samtidigt blir cyberbrottsligheten alltmer industrialiserad med specialiseringar och innovativa tjänster på darknet. Ökade geopolitiska motsättningar höjer dessutom risken för statsstödda attacker mot vårt samhälle.

Sammanfattningsvis visar analysen att den kriminella miljön ständigt förändras, och att risken för mer sofistikerade brott ökar. Även om myndigheter, näringsliv och individer alla måste samarbeta för att begränsa skadeverkningarna, är kunskap och information en viktig första försvarslinje. Med denna rapportserie vill vi bidra till ökad förståelse och medvetenhet hos både allmänhet och mindre företag, så att de kan förbereda sig bättre på de hot och utmaningar som väntar.

Introduktion av brottsmarknaden

Inledning – en omfattande kriminell verklighet

Brottsligheten har utvecklats till en global, komplex och omfattande kraft i vår tid. Globalisering, tekniska framsteg och digitala miljöer öppnar nya vägar för kriminella nätverk att växa, organisera sig och agera över nationsgränser.

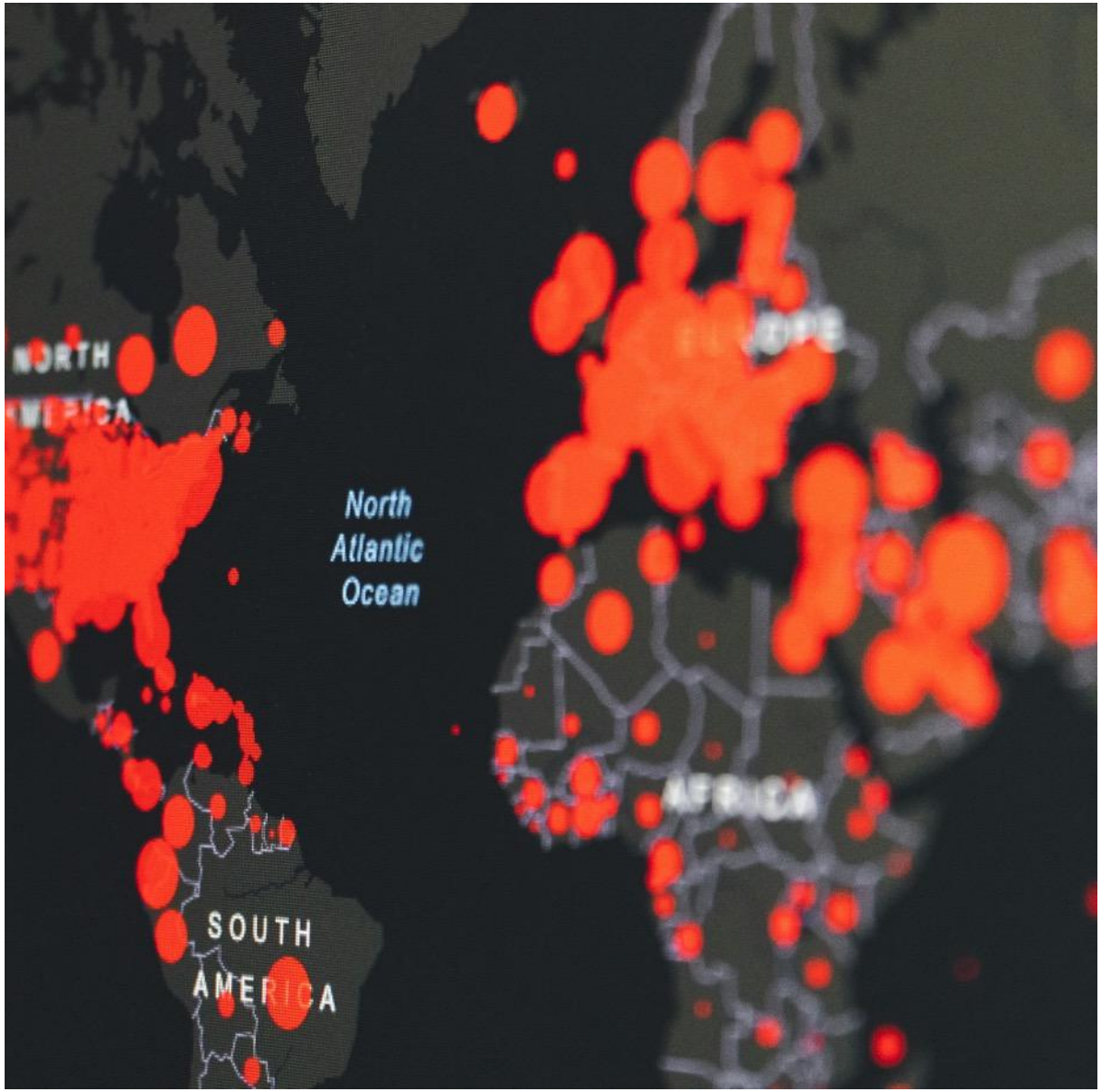
För att förstå denna dynamiska spelplan har vi kartlagt de centrala kriminella spelarnas organisering, verksamhetsområden och drivkrafter. Genom intervjuer med experter med olika perspektiv har vi samlat insikter om hur dessa krafter fungerar, hur de påverkar Sverige och vilka områden som kan kräva särskild uppmärksamhet framöver.

I rapporten undersöker vi hur den kriminella ekonomins strukturer och vad som driver den. Vi belyser också hur nätverken förändras, anpassar sig och ständigt hittar nya vägar till ekonomisk vinning och andra mål – samtidigt som gränserna mellan ekonomiska brott och politiskt eller socialt motiverade handlingar gradvis suddas ut.

Vår utgångspunkt är att betrakta kriminella nätverk ur ett marknadsperspektiv, där de kontinuerligt söker nya möjligheter att växa och begå brott mot samhället, dess invånare och företag – i stället för att fokusera på hur rättsväsendet försöker bekämpa dem.

Det ligger i brottslighetens natur att kriminella aktörer försöker dölja sina aktiviteter, vilket försvårar kunskapsinhämtningen. Den information vi har lyckats samla ger ändå en övergripande bild – om än inte en heltäckande sådan.

Vårt syfte är därför inte att skapa en total översikt av den kriminella spelplanen, utan att ge en bild av nuläget, visa vart brottsligheten kan vara på väg och peka på områden som kräver särskild uppmärksamhet för att stärka skyddet mot brott. Genom att analysera dessa krafter ökar vi vår beredskap inför framtidens brottslighet: ju bättre vi förstår motståndaren, desto bättre rustade är vi att motverka dess framfart.



Digitaliseringen skiftar vardagsbrottslighetens fokus: färre stölder, fler digitala bedrägerier

Minskning av stölder i fysiska miljöer

Antalet polisanmälda *stölder och andra tillgreppsbrott*[1] har minskat med 42 procent under de senaste 20 åren. År 2023 registrerades 381 041 tillgreppsbrott, vilket är en betydande minskning från 651 749 anmälningar år 2004.

Under samma period har antalet anmälda *inbrottsstölder*[2] också minskat med 42 procent, varav *bostadsinbrotten*[3] minskade med 38 procent. Denna trend är inte unik för Sverige utan speglas även i andra höginkomstländer.

Forskning pekar på att förbättrade säkerhetsåtgärder är en viktig förklaring till denna utveckling. Exempelvis har elektroniska startspärrar i fordon och moderniserade säkerhetssystem i hemmen försvårat för kriminella att genomföra tillgreppsbrott. Den tekniska utvecklingen och ökad medvetenhet hos allmänheten har därmed haft en märkbar brottspreventiv effekt.

Digital brottslighet på frammarsch

Brottsligheten i digitala miljöer fortsätter att öka, vilket främst kan tillskrivas de nya möjligheter som digitaliseringen och internet skapat för kriminella aktörer. Denna utveckling tycks inte drivas av att traditionella inbrottstjuvar bytt fokus, utan av en växande arena för nya typer av brott.

Bedrägeribrott är ett av de mest framträdande exemplen på digital brottslighet. Ökningen drivs särskilt av möjligheten att genomföra bedrägerier via digitala kanaler, som e-post, sms och sociala medier. Metoder som phishing, kortbedrägerier och identitetsstölder gör det möjligt att rikta attacker mot många individer samtidigt, vilket gör dessa brott lönsamma. Digitaliseringens framväxt har därmed skapat nya och effektiva arenor för brottslighet.

Polisanmälda bedrägeribrott[4] har ökat kraftigt de senaste tio åren, från 156 087 anmälningar år 2014 till 238 371 år 2023, vilket motsvarar en ökning på 53 procent.

Dessa brott har blivit en del av det vi benämner vardagsbrott, där mängder av individer och företag riskerar att drabbas i sin vardag.

[1] Brå, BrB 8 kap. totalt. [2] Brå, Inbrottsstöld, inte av skjutvapen, totalt. [3] Brå, Inbrottsstöld i bostad (lägenhet, villa) [4] Brå, Bedrägeri och annan oredlighet, totalt

Den kriminella ekonomin i Sverige omsätter 100-150 miljarder kronor

Den förändrade kriminella spelplanen i Sverige

Den kriminella spelplanen i Sverige har förändrats dramatiskt under de senaste decennierna. Det som en gång var en relativt isolerad och lokal företeelse har nu utvecklats till komplexa och internationella nätverk. Idag suddas gränserna mellan olika typer av brottslighet ut, där både så kallade vardagsbrott – som inbrott i bostäder, stöld av fordon och cyklar – och grova brott som narkotikahandel, ekonomisk brottslighet, cyberbrott på hög nivå och våldsbrott kopplade till organiserad brottslighet, utförs med en allt högre grad av organisering och samverkan.

Sverige som en del av den globala kriminella ekonomin

Den kriminella ekonomin i Sverige begränsas inte till brott som utförs av inhemska aktörer. Tvärtom påverkas den starkt av internationella nätverk och gränsöverskridande brottslighet. Verksamheter som narkotikahandel, människosmuggling och cyberbrott drivs ofta av globala organisationer med bas utanför Sveriges gränser, men får ändå ekonomiska och sociala återverkningar i landet. Därför är Sveriges kriminella ekonomi en integrerad del av ett större internationellt ekosystem.

Professionalisering och digitalisering

Idag präglas brottsligheten av en allt högre grad av professionalisering och digitalisering. Traditionella gatugäng samverkar med både cyberbrottslingar och internationella kriminella nätverk, vilket bidrar till den kriminella ekonomins uppskattade omsättning på 100–150 miljarder kronor årligen i Sverige. Detta är i nivå med den globala omsättningen hos några av Sveriges största industrikoncerner, som Electrolux – en av världens största tillverkare av hushållsapparater – samt industrikoncernen Sandvik och bygg- och projektutvecklingsbolaget Skanska. Detta illustrerar den organiserade brottslighetens omfattande ekonomiska inflytande. För att sätta siffran i ytterligare perspektiv kan det jämföras med Sveriges försvarsbudget år 2024, som uppgår till 119 miljarder kronor.

Den kriminella världen: Professionaliserad, globaliserad och bättre organiserad

62 000 människor är kopplade till kriminella nätverk i Sverige

I Sverige finns det flera stora kriminella nätverk som utgör ett allvarligt samhällsproblem. Enligt Polismyndigheten är cirka 14 000 personer aktiva i kriminella nätverk, och ytterligare 48 000 har kopplingar till dem. 88 procent av de aktiva är svenska medborgare. Nätverken är ofta inblandade i narkotikasmuggling och distribution, en av de mest utbredda kriminella verksamheterna. Polisen uppskattar att omkring 600 personer styr grov organiserad brottslighet i Sverige från 57 andra länder.

Rekrytering sker i allt yngre målgrupper

Kriminella nätverk i Sverige rekryterar allt yngre personer, ofta barn och ungdomar, för att bygga ut sina distributionskedjor för narkotika. Rekryteringen sker genom att äldre tonåringar lockar in yngre barn, vilket skapar en hierarkisk struktur inom nätverken. Dessa nätverk är inte bara lokala utan har även nationella och internationella kopplingar, vilket gör dem svåra att bekämpa. Enligt polisens rapporter är 5 400 personer under 18 år kopplade till nätverken.

Globalisering av kriminaliteten

Kriminalitet har gått från att vara lokal till att bli global. De mest kända fallen av internationell brottslighet involverar stora, inflytelserika organisationer som opererar över nationsgränser. Med teknik som mobiltelefoner och datorer kan brott nu organiseras och utföras över hela kontinenter. Dessa organisationer är kända för sin förmåga att anpassa sig och dra nytta av globala, ekonomiska och teknologiska förändringar för att expandera sin verksamhet.

För att effektivt genomföra sina operationer etablerar de ofta kontakter med lokala kriminella grupper, som de utnyttjar som utförare. Detta nätverk av lokala partners gör dem svåra att bekämpa på internationell nivå. Europol har kartlagt över 800 kriminella nätverk i EU, vilket visar att dessa nätverk är mycket anpassningsbara och opererar på ett sätt som liknar internationella företag.

Mångsidig kriminalitet

Mäktiga kriminella grupper ägnar sig ofta åt en rad olika brott, såsom narkotikahandel, penningtvätt, cyberbrott, utpressning, bedrägerier, vapensmuggling och människohandel. Denna diversifiering minskar riskerna, stärker kärnverksamheten och ökar vinsterna. Nätverken opererar dessutom alltmer som företag, med tydliga hierarkier, roller och specialiseringar, vilket gör det möjligt för dem att effektivisera och maximera sina intäkter genom att tillämpa affärsmodeller inom sina verksamheter.

Polismyndigheten och Brottsförebyggande rådet belyser hur dessa nätverk anpassar sig efter marknadsförhållanden och använder strategier för att optimera sin brottsliga verksamhet. På så sätt utnyttjar de ekonomiska möjligheter för att stärka och expandera, vilket ytterligare understryker deras företagsliknande struktur.

Möjliggörare i näringslivet stärker kriminella

Kriminella nätverk i Sverige har utvecklats mot att operera som företag, med tydliga hierarkier, roller och specialiseringar. Denna struktur möjliggör effektivisering och maximering av intäkter genom att tillämpa affärsmodeller inom kriminella verksamheter. En viktig del i detta är olika typer av ”möjliggörare”- personer som underlättar verksamheten genom exempelvis penningtvätt eller logistik. Det kan handla om jurister, revisorer eller andra med förtroendeingivande roller i samhället.

”Från den tunna röda linjen, till den tunna blå linjen, till Cyber Blue Line: Var ligger ansvaret nu när det gäller att upprätthålla säkra samhällen i cyberrymden?”
Europol.

Nätpatrullering

Poliserna i Region nord patrullerar på nätet för att upptäcka och utreda brott.
– Ökar vi vår närvaro på nätet får vi bättre förutsättningar att förebygga brott, men även upptäcka och utreda brott, säger John Forsberg.
Källa: SVT Nyheter

” Inom polisen talar vi ofta om utsatta, socialt utsatta och särskilt utsatta områden. Nu är det den digitala miljön som är vårt särskilt utsatta område – som fortfarande är obemannat,” *John Forsberg*.

John Forsberg *är chef för utvecklingscentrum Nord, Nationella operativa avdelningen (NOA) inom Polismyndigheten. Här arbetar han arbetar med att utveckla och implementera Polismyndighetens brottsbekämpande arbete både fysiskt och digitalt för ett tryggare och säkrare Sverige och Europa. Forsberg har förutom en lång karriär inom polisen även arbetet som expert i flertalet statliga utredningar. Forsberg är aktuell i ett nytt initiativ där polisen har börjat patrullera på nätet för att upptäcka och förebygga brott.*

Polisiär digital närvaro

Den digitala och fysiska världen är nu tätt sammanflätade, och det ställer helt nya krav på polisens förmåga att agera i båda miljöerna. Forsberg menar att när polisen inte är närvarande i den digitala miljön skapas en känsla av ett laglöst samhälle på nätet, där kriminella aktörer kan agera fritt och ostört. Det handlar inte bara om att polisen ska vara tillgänglig för interaktion, utan också om att agera proaktivt och avvärja brott innan dem sker i dessa miljöer. Genom att upprätthålla digital närvaro kan polisen bygga förtroende och säkerställa att brott inte får fäste i miljöer där medborgarna tillbringar alltmer tid. En utmaning för polisen är att man saknar motsvarande rättigheter att agera i digitala världen som i den fysiska.

Spelmiljöer som grogrund för kriminalitet

Forsberg beskriver hur det i spelmiljöer, där mycket interaktion sker, är vanligt att kriminell aktivitet blomstrar. Kriminell kommunikation, rekrytering och radikalisering kan ske inom dessa miljöer, där det också finns potential för brottsförebyggande arbete. Medborgare är aktiva i den digitala världen, och vi måste utveckla strategier för att möta dessa nya hot. Ett exempel är Roblox, med över 200 miljoner aktiva användare varje månad, som är en av världens största spelplattformar. Här förekommer exempelvis bedrägerier där användare luras på värdefulla föremål, såsom skins. Men här sker även grooming och radikalisering av unga.

Kriminalitetens internationella kopplingar

Kriminell verksamhet i Sverige har allt oftare internationella kopplingar. Ett lokalt brott, som en skjutning, kan ofta spåras till internationella nätverk. Forsberg resonerar kring hur en anstiftare i, låt säga, ett land som Turkiet kan skicka en order till en kriminell i en stad som Stockholm, som i sin tur anlitar en utförare från exempelvis ett HVB-hem i en mindre ort, som Kalix. Vapnen kan fraktas från andra orter i landet, och nätverken använder lokala ankarplatser för att samla gods, vila och planera vidare brott. Den här globala kopplingen ställer helt nya krav på rättsvårdande myndigheter.

Brottsligheten bör idag benämnas - *glokal*.

Allianser mellan statsaktörer och kriminella

En oroande utveckling enligt Forsberg, är samarbetet mellan statsaktörer och organiserad brottslighet. Det finns risk för att ohederliga allianser blir allt vanligare, där båda parter drar nytta av varandra för sina respektive syften. Ett skrämmande exempel är när statsaktörer kan skicka svenska ungdomar för att utföra politiska handlingar, som att attackera en ambassad. Den här växelverkan mellan stat och kriminalitet utgör ett stort säkerhetsproblem, både för företag och enskilda individer i Sverige.

Klimatförändringar påverkar brottslighet

Ett par fenomen som Forsberg menar banar väg för nya typer av brottslighet och som vi pratar för lite om, är klimatförändringarna och miljöförstöring. Effekterna av klimat- och miljöförändringar kommer inte bara att påverka ekosystemen och människors livsvillkor, utan också skapa möjligheter för kriminella aktiviteter, där resurser som människor och avfall alltmer blir föremål för exempelvis illegal handel. Klimatförändringar kan tvinga människor på flykt och skapa en grogrund för människohandel och smuggling. Kopplingen mellan klimatkris och brottslighet är tydlig, och det är viktigt att vi diskuterar och arbetar med dessa frågor

Kriminella nätverk använder vanliga företag som täckmantel

Kriminella nätverk integreras allt oftare med vanliga företag

Kriminella nätverk har alltmer börjat organisera sig med en företagsliknande struktur för att effektivisera sina operationer och dölja den illegala verksamheten. Genom att använda företag som fasad kan de smidigt maskera brottsliga aktiviteter som penningtvätt och bedrägerier under en skenbart legitim yta. Denna strategi gör det möjligt för dem att verka mer obemärkt och samtidigt utnyttja samhällets ekonomiska och administrativa system.

Denna typ av organiserad brottslighet utgör ett hot mot samhällets motståndskraft och ekonomiska stabilitet. Det påverkar inte bara seriösa företag utan utsätter också enskilda individer för exploatering, bland annat genom identitetsstöld och falska inkomstuppgifter.

Ekonomisk vinning är en stark drivkraft och kriminella rör sig ofta i en gråzon mellan laglig och olaglig verksamhet. Svarta löner har delvis övergått till låga, vita löner, samtidigt som exploatering av arbetskraft och falska löneuppgifter förekommer.

Företag som styrs av kriminella kan verka lagliga inom en rad olika branscher, men fungerar i själva verket som en täckmantel för brottsliga syften. Genom dessa företag kan kriminella exempelvis importera arbetskraft från tredjeland, ansöka om bidrag och utnyttja det svenska skattesystemet på olagliga sätt.

Majoriteten av Europas farligaste kriminella nätverk använder legala verksamheter

Majoriteten av de mest samhällsfarliga kriminella nätverken i Europa använder legala verksamheter för att bedriva brottslighet. Enligt Europol använder hela 86 procent av dessa nätverk lagliga företag som täckmantel för sin kriminalitet.

– EU:s inre säkerhet är hotad, varnar Europolchefen Catherine De Bolle. Nätverken infiltrerar existerande företag eller startar egna verksamheter. Några av de mest utsatta sektorerna är transport, byggsektorn och besöksnäringen. Legala verksamheter används också för penningtvätt, där Europol pekar ut fastighetsinvesteringar, detaljhandel med dyra varor och företag med mycket pengar i omlopp.

Organiserad brottslighet innebär miljardförluster för staten och hotar både invånarnas trygghet, säkerhet och hälsa samt samhällsviktiga funktioner, demokratin och rättssäkerheten.

– Den grova brottsligheten har gått från att råna banker och värdetransporter till att nu råna socialförsäkringen istället. Vi måste bygga system som klarar den typen av påfrestningar och förhindra att brotten kan begås. För att göra det behöver vi kunna byta information som är viktig för brottsbekämpning mellan myndigheter på ett bättre sätt. Informationen finns, men den är inte tillgänglig, säger Britt-Marie Hultström, verksamhetsområdeschef, Försäkringskassan.

Enligt Europol har en tredjedel av de 821 samhällsfarliga nätverken varit aktiva i mer än 10 år. Deras överlevnad hänger ofta samman med hur framgångsrika de är i att kontrollera legala företag.

Adena Friedman

Chair & CEO, Nasdaq

"If financial crime were a sector of the U.S. economy, it would be on par with the lodging and food services sector—with money laundering activity accounting for 3.1% of national GDP in 2023. The world's multi-trillion-dollar financial crime epidemic is more than a money problem."

Kriminella organisationer smälter in i samhället – och har kontakter och inflytande på hög nivå

Bildkälla: BBC

”Jag tror att man har underskattat vidden av nätverken och deras kontakter. Ledarskikten kan ha kontakter med högt uppsatta personer runt om i världen,” säger ***SVT:s kriminalreporter*** *Sofia Yohannes om den senaste skottlossningen vid Israels ambassad I Stockholm och att Foxtrotnätverket påstås agera på uppdrag av Iran.*

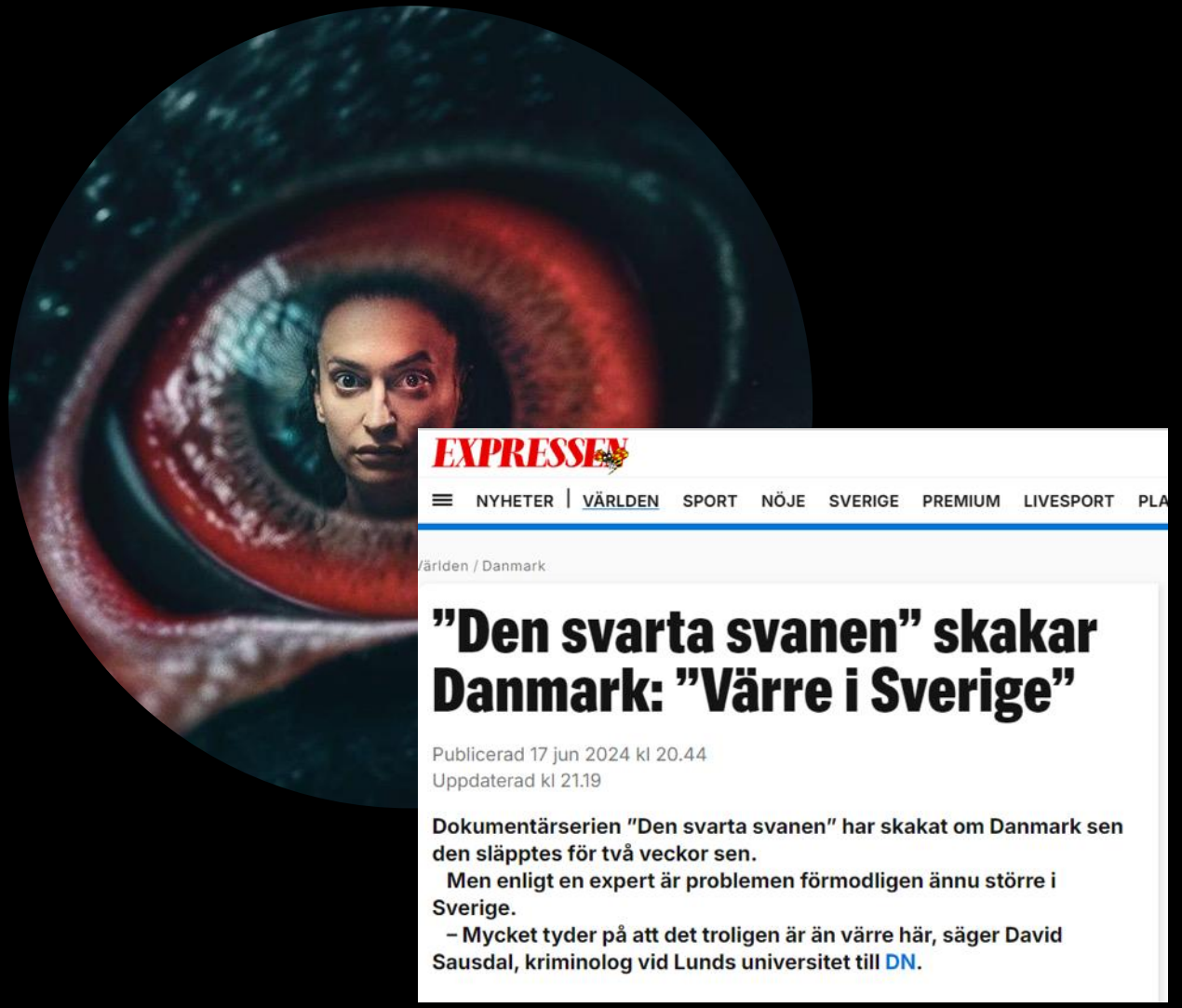
Ur SVT artikeln 241003 "Uppgifter: Dåd mot ambassader i Stockholm och Köpenhamn ska ha utförts på uppdrag av Foxtrot”

”Maffianätverk förändras tillsammans med resten av samhället. De börjar i allt högre grad se ut som resten av oss,” säger Nicola Gratteri, italiensk åklagare. ”Men trots att 'Ndrangheta blivit en toppmodern organisation är dess medlemmar lika redo att ta till extremt våld som tidigare.”

Ur YLE artikeln 210113 "Italien inleder massrättegång mot Europas mäktigaste kriminella – 'Ndrangheta-maffian tros vara rikare än Deutsche Bank och McDonalds tillsammans.”

”Genom att använda företag som brottsverktyg får man tillgång till den legala sfären och kan utnyttja detta till att begå brott som t.ex. bedrägerier och brott mot välfärdssystemet. Huvudmännen kan undgå straff genom att sätta in målvakter som företrädare för företaget…” säger Torbjörn Rosén, polischef vid Ekobrottsmyndigheten.

Ur Ekobrottsmyndighetens artikel 211020 ”Kriminella företag utnyttjar de svenska välfärdssystemen”.



Bildkälla: SVT

Påverkan och utmaningar

Internationella kriminella nätverk påverkar oss i Sverige på flera sätt

Ökad otrygghet och rädsla

Kriminella nätverk har en påtaglig inverkan på invånarnas vardagsliv i Sverige. Våldsamma uppgörelser mellan rivaliserande grupper skapar oro och leder till att många känner sig otrygga i offentliga miljöer. Utpressning och hot, både mot privatpersoner och företagare, förstärker rädslan och gör att vissa människor väljer bort platser eller ändrar sina vardagsrutiner av säkerhetsskäl.

Påverkan på lokalsamhällen

I många bostadsområden märks den kriminella närvaron genom exempelvis narkotikaförsäljning, vilket minskar tryggheten för de boende. I takt med att kriminalitet ökar kan områden stigmatiseras och förlora i anseende, något som i sin tur försämrar livskvaliteten för invånarna.

Infiltration av företag och hot om våld

Kriminella nätverk utnyttjar företag på flera sätt, exempelvis genom att tvätta pengar eller kringgå lagstiftning bakom en legitim fasad. Samtidigt kan företag utsättas för hot och utpressning när de inte samarbetar med kriminella aktörer, vilket leder till en otrygg arbetsmiljö och pressade beslut som gynnar nätverken.

Säkerhetsrisker och ökade kostnader

Det rådande säkerhetsläget gör företag i Sverige, liksom i övriga Europa, mer sårbara för angrepp från kriminella. För att skydda sig krävs ofta dyra säkerhetsåtgärder, vilket särskilt drabbar mindre företag. Även privatpersoner blir allt försiktigare och kan tvingas lägga tid och pengar på att öka sin trygghet, till exempel genom försäkringar eller säkerhetslösningar.

Ekonomiska konsekvenser

Den organiserade brottsligheten skapar stora samhällskostnader. Välfärdsbrott urholkar samhällets skyddsnät. Skattebrott minskar statens inkomster och påverkar kvaliteten på välfärden, medan arbetslivskriminalitet – exempelvis genom människohandel och svartarbete – leder till osunda arbetsvillkor och snedvriden konkurrens för seriösa företag.

Digitala risker och hot

I den digitala sfären har cyberbrott blivit allt vanligare. Kriminella nätverk använder dessutom avancerade metoder för dataintrång eller spridning av skadlig kod. Detta skapar oro och kräver ökade investeringar i säkerhet, både på individ- och företagsnivå.

Systemhotande verksamhet

Kriminella nätverk begränsar sig inte till enskilda företag eller lokala områden. I en tid av ökade geopolitiska spänningar och antagonism från främmande makter kan deras aktiviteter även flätas samman med illvilliga staters intressen. Resultatet blir inte bara våld och hot i lokalsamhällen eller rekrytering av unga till kriminella kretsar, utan också sabotage mot kritisk infrastruktur och attacker mot samhällets institutioner. Detta undergräver förtroendet för myndigheter och bidrar till en ökad instabilitet på nationell och internationell nivå.

Samarbete för att möta hoten

För att motverka dessa omfattande utmaningar arbetar svenska myndigheter aktivt för att stärka det internationella brottsförebyggande samarbetet. Målet är att förhindra och försvåra den gränsöverskridande brottslighet som riktar sig mot Sverige.

”När vi pratar säkerhet utifrån mänskliga aspekter, så gör vi det ofta som om tekniken vore någon form av naturlag”, *Joakim Kävrestad*.

Joakim Kävrestad *är en svensk akademiker och expert inom informationsteknologi, med en särskild inriktning på digital forensik och IT-säkerhet. Han arbetar som lektor vid Tekniska Högskolan i Jönköping, där han undervisar inom IT-området. Kävrestad har en doktorsexamen i informationssäkerhet och har tidigare arbetat som digital forensiker för den svenska polisen. Utöver sin undervisning är han författare till flera läroböcker inom sitt expertområde. Han är även engagerad i forskningsprojekt som syftar till att motverka digital kriminalitet.*

Vi har försummat att utveckla säkra system

Trots att digitaliseringen genomsyrar hela vårt samhälle har vi misslyckats med att bygga säkra system från grunden. Samhället har valt att hantera problem med tillfälliga lösningar snarare än att ta itu med grundproblemen, enligt Kävrestad. Så länge marknaden själv ska ansvara för att säkerställa trygga köp för konsumenterna, kommer vi inte att lösa de underliggande problemen. För att uppnå verklig säkerhet krävs lagstiftning, menar Kävrestad. Han poängterar även att vi som samhälle måste reflektera över vilken grad av hot vi är villiga att acceptera.

Vidare reflekterar Kävrestad hur samhället har misslyckats med att utbilda allmänheten om vikten av att skydda sig mot digitala brott. Perspektivet att först skapa system och sedan lägga till en grundläggande säkerhet måste omvärderas. Användarcentrerad design kan vara en nyckel till framtida lösningar. Kävrestad betonar att människor måste förstå att all data, även din egen, är värdefull för någon. Han ger exempel på hur hackare kan ta över ett Facebook-konto för att lura till sig pengar genom bedrägerier. Genom att använda det stulna kontot kan de utnyttja offrets nätverk för egen vinning, till exempel genom att skaffa sig något de vill ha – en pryl eller annan tillgång – utan att hackaren själv står för kostnaden.

Övervakning eller anonymitet?

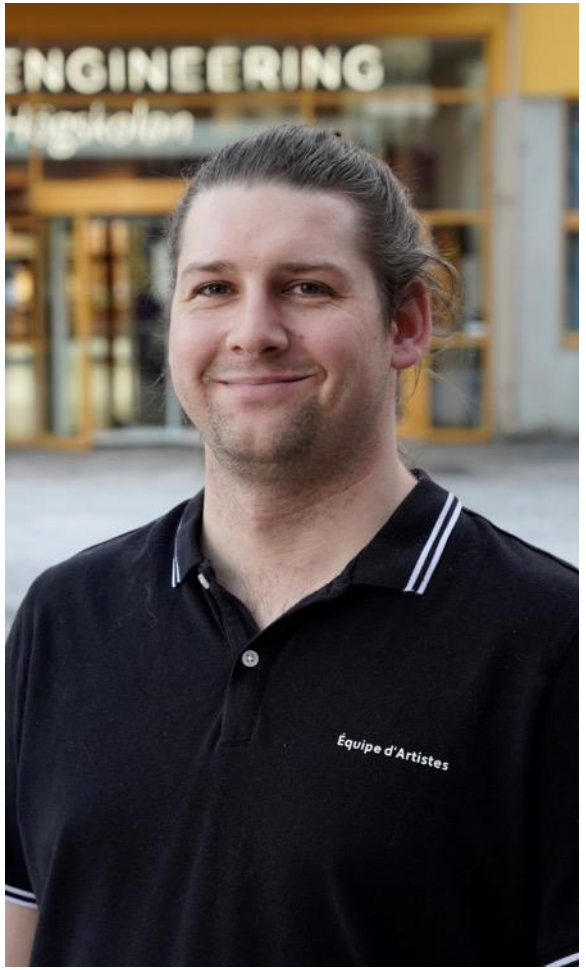
Insamling av människors identitet för att lagra i en stor databas kan vara rimligt, men bara om vi kan lita på den aktör som har nyckeln till databasen till 100%. Och att informationen endast hämtas ut med till exempel tingsrättens godkännande. Utmaningen ligger i att hitta en "key keeper" som alla kan lita på fullt ut. Ett EU-lagförslag som har mött kritik för risken att leda till massövervakning av alla medborgares kommunikation är Chat Control. Förslaget syftar till att bekämpa spridning av material med sexuella övergrepp mot barn online, tillåter övervakning av meddelanden, även krypterade sådana. Denna slags övervakning menar Kävrestad kan potentiellt försvaga tryggheten snarare än att stärka den, då risken är stor att någon missbrukar en bakdörr.

"Vilda västern" när internet växte fram

Kävrestad berättar att i internets tidiga dagar var det en ung generation som "härjade fritt" på nätet, skyddade av anonymitetsverktyg och bristande regleringar. Internet växte snabbt, och samhället hade svårt att hänga med i att skapa lagar och regler för den nya digitala miljön. Lagstiftningen försöker nu att komma ikapp, men för vissa som tidigare laddade ner olagligt material kvarstår en känsla av att det borde vara tillåtet, som om det vore ett privilegium de fortfarande har rätt till. Kävrestad menar att det finns en grupp som inte ser sig själva som kriminella, utan som "bara" balanserar på moralens gräns.

Digitala forensik spårar brottslingar i "offline-brott"

En fråga som Kävrestad är mycket engagerad i är hur den digitala utvecklingen inte bara blir ett verktyg för kriminella, som vid hacking eller nätbedrägerier, utan också ett kraftfullt hjälpmedel för rättsväsendet. Genom teknologin i våra mobiltelefoner kan traditionella brott i allt högre grad bevisas. Nästan alla bär med sig en mobiltelefon, och enbart genom dess närvaro kan vi ofta positionera den, och därmed potentiellt också personen. Om vi dessutom lägger till information om korttransaktioner kan vi få en bra uppfattning om var en individ befunnit sig, till exempel under en kväll ute. Genom att kombinera detta med sökhistorik kan vi bygga en beviskedja som tidigare inte varit möjlig. Tyvärr saknas det fortfarande tillräcklig kunskap hos en stor del av polisen och utredarna, vilket begränsar möjligheten att fullt ut utnyttja digital forensik i fler fall.



Spelplanen

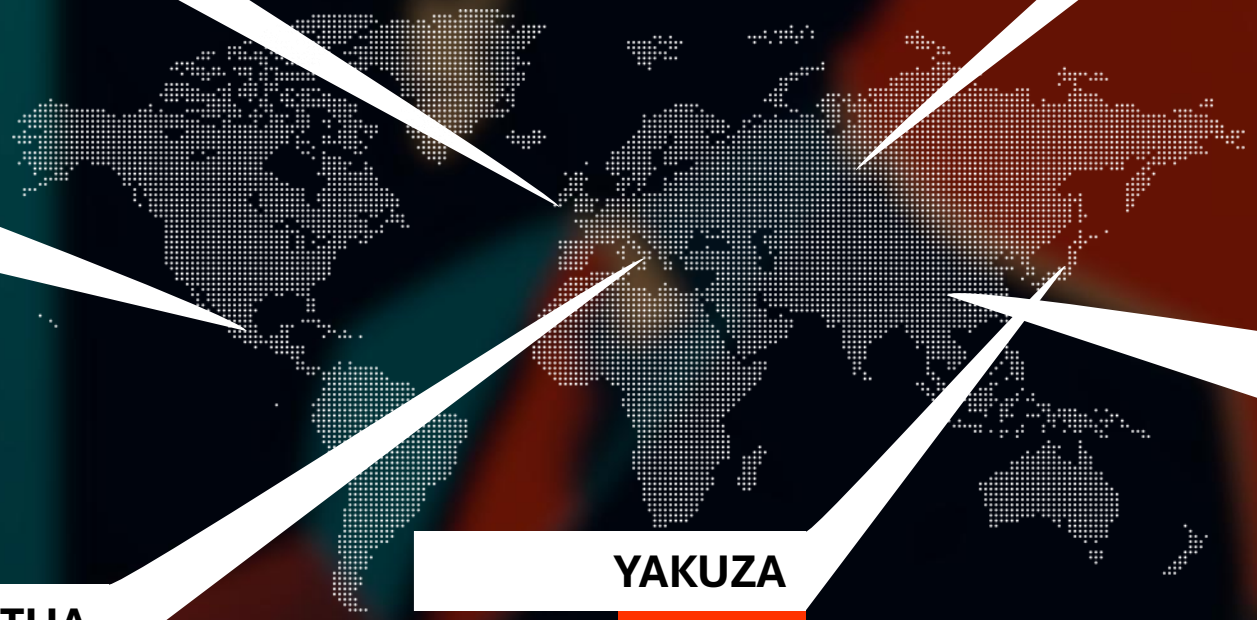
The Old Big Crim

The Old Big Crim utgörs av traditionella kriminella nätverk som har utvecklats under lång tid och som kännetecknas av komplexa hierarkier och djupa rötter i samhället, där de byggt upp makt genom lojalitet, våld och omfattande kontroll över samhällen via ekonomiskt inflytande och korruption. I de flesta av dessa organisationer är narkotikasmuggling central. Exempel på sådana nätverk är 'Ndrangheta, Sinaloakartellen, Yakuza, Triaderna och Ryska maffian. Dessa grupper har inte bara expanderat internationellt, utan också förfinat sina verksamheter genom att komplettera sin kärnkriminalitet med andra brottstyper som stödjer och maskerar huvudaffärerna.

Genom att anpassa sig till globalisering och teknologisk utveckling har de blivit alltmer digitala och använder legala företag som täckmantlar för att legitimera och skydda sina brottsliga aktiviteter, vilket stärker deras inflytande. Trots strängare lagar och ökat myndighetstryck som har begränsat deras makt på vissa områden, fortsätter dessa nätverk att utveckla nya affärsmodeller för att bibehålla sin ställning i en föränderlig värld.

The Old Big Crim

Exempel på internationellt mäktiga nätverk



KINAHAN
IRLAND

Från gatugäng till internationell drogkartell.

SINALOA
MEXICO

Står för 40-60% av droghandeln i Mexiko med vinster på 3 miljarder dollar.

NDRANGHETHA
ITALIEN

Det mäktigaste kriminella nätverket i Italien.

YAKUZA
JAPAN

Japans traditionella nätverk förlorar makt, men fortsätter existera i nya konstellationer.

RYSKA MAFFIAN
RYSSLAND

En komplex och ibland otydlig relation mellan den ryska maffian och statliga institutioner, ”en ohelig allians”.

TRIADERNA
KINA

Triaderna har expanderat globalt och etablerat en starkare närvaro i många med tillgång till nya marknader och inkomstkällor.

The New Big Crim

Cyberattacker med Avancerad Teknisk Kompetens

Cyberbrottslighet för finansiell vinning

Cyberattacker för politiska och sociala ändamål

The New Big Crim

En ny typ av globala, tekniskt avancerade kriminella nätverk uppstod i svallvågorna av digitaliseringen och särskilt efter lanseringen av smartphones världen över. Dessa angripare utnyttjar cyberattacker, ransomware och finansiella bedrägerier för att stjäla pengar och data samt skada nationer, företag och individer.

I rapportens analys identifieras tre kategorier av The New Big Crim: ”Cyberattacker med avancerad teknisk kunskap”, ”Cyberbrottslighet för finansiell vinning” och ”Cyberattacker för politiska och sociala ändamål”. Gränserna mellan kategorierna är flytande och vissa kriminella grupper passar in på fler kategorier.

The New Big Crim utgörs ofta av flexibla och löst sammansatta grupper som samverkar kring brott i digitala miljöer. Grupperna är flyktiga och undviker att skapa igenkännbara identiteter vilket gör dem svårare att spåra. De bildas, upplöses och återuppstår i nya konstellationer utan långsiktig struktur på motsvarande vis som Old Big Crim. Deras medlemmar samlas kring specifika brottsverktyg och engagerar sig ofta i lösa eller tillfälliga samarbeten.

För att möta behovet av att identifiera befintliga och nya cyberkriminella grupper har säkerhetsföretag och myndigheter utvecklat olika namnsystem. Vissa använder APT-beteckningar (Advanced Persistent Threat), andra djurnamn, exempelvis björn för ryska aktörer eller panda för kinesiska, och mytologiska väsen som Chollima för nordkoreanska grupper. Ibland numreras grupper efter upptäckt, och samma grupp kan få flera namn beroende på vem som döpt dem, som exempelvis APT28 och Fancy Bear.

Men vissa cyberkriminella grupper väljer en annan strategi. Genom att aktivt bygga varumärken och skryta om sina attacker hoppas de vinna anseende i den kriminella världen. Detta självförhärligande kan dock leda till sårbarheter. *Lockbits* aggressiva profilering kan ha varit en bidragande faktor till att de nyligen spårades och neutraliserades. Detta visar på riskerna med offentlig exponering i en annars dold skuggvärld. Trots dessa tillslag är landskapet i ständig förändring. Nya grupper bildas och gamla omorganiseras, vilket ställer krav på rättsväsendets kontinuerliga bevakning och proaktiva motåtgärder.

Bakom många av dessa kriminella grupper står stater som skyddar eller tolererar deras aktiviteter för att uppnå egna strategiska mål. Genom att blunda för eller stödja dessa handlingar kan stater dra nytta av attacker mot andra nationer för att försvaga deras infrastruktur eller stjäla känslig information. I vissa fall styr statliga aktörer aktivt gruppernas handlingar för cyberspionage, sabotage, politisk påverkan eller ekonomisk vinning. Detta suddar ut gränsen mellan organiserad brottslighet och statligt sanktionerade operationer och skapar ett alltmer komplext hotlandskap.

Cyberattacker med avancerad teknisk kompetens

Sofistikerade och Globala Cyberkriminella Grupper

I denna kategori återfinns så kallade Advanced Persistent Threats (APT), där grupper med betydande resurser och teknisk spetskompetens genomför strategiska och ofta långsiktiga infiltrationer av IT-system. Även om de sällan riktar sig direkt mot allmänheten kan deras attacker ändå få omfattande konsekvenser genom att stjäla känslig information, störa samhällsviktiga verksamheter eller sabotera kritisk infrastruktur.

Exempel på sådana grupper finns i flera länder. *APT32*, med kopplingar till Vietnam och känd sedan 2014, bedriver cyberkriminalitet och gör dataintrång mot mål som high-tech bolag, sjukvård, tillverkningsindustrin och fientliga stater. En annan framträdande aktör är *AlphV/BlackCat,* som nyttjar en bred arsenal av tekniker – från nätfiske och skadliga e-postbilagor till utnyttjande av kända sårbarheter – för att få initial åtkomst till system. Deras anpassningsförmåga gör dem till en viktig spelare i det växande Ransomware-as-a-Service (RaaS)-ekosystemet.

På den statliga arenan finns till exempel *APT41* från Kina, som kombinerar spionage med cyberbrottslighet och snabbt anpassar sina avancerade metoder till nya säkerhetsåtgärder. *Lazarus Group*, med kopplingar till Nordkorea, är känd för aggressiv ekonomisk brottslighet och destruktiva attacker, ofta i linje med landets intressen. Rysslandsbaserade *APT28* (även känd som Fancy Bear, Sofacy eller Forest Blizzard) angriper sektorer som utrikesfrågor, försvar och offentlig förvaltning, medan *APT29* (Cozy Bear, Nobelium eller Midnight Blizzard), även den kopplad till Ryssland, riktar in sig på IT-tjänster och offentliga institutioner. Den senare gruppen gömmer ofta sin skadliga trafik bakom legitima molntjänster, vilket gör den särskilt svår att upptäcka.

Dessa exempel illustrerar hur APT-grupper, oavsett om de drivs av ekonomiska, politiska eller strategiska motiv, utgör ett komplext och föränderligt hot mot både privata och offentliga aktörer världen över.

Cyberbrottslighet för finansiell vinning

Ekonomiskt Drivna Cyberhot: Ransomware-as-a-Service

Denna kategori av cyberbrottslighet präglas av grupper vars främsta drivkraft är ekonomisk vinning. Angreppsmetoderna varierar och omfattar allt från traditionella phishingmejl och skadlig programvara till avancerade attacker mot leverantörskedjor. Ett centralt inslag är Ransomware-as-a-Service (RaaS), där tekniskt kunniga utvecklar och förädlar ransomware-verktyg, som de sedan erbjuder till andra kriminella via dolda handelsplatser på nätet. På så vis sänks tröskeln för nya aktörer att ge sig in i den brottsliga verksamheten, vilket i sin tur breddar kretsen av potentiella angripare och gör attackerna svårare att förutse och stoppa.

Akira, Clop och *AlphV/BlackCat* är exempel på brottsliga cybergrupper som drivs av ekonomisk vinning. De infiltrerar nätverk, stjäl och krypterar data för att sedan kräva lösensummor för att låsa upp systemen eller förhindra läckage av känslig information. Dessa utpressningsattacker kan slå hårt mot både företag och privatpersoner, och RaaS-modellen underlättar spridningen av denna typ av brottslighet genom att fler, mindre tekniskt kunniga aktörer får tillgång till färdiga verktyg.

Vissa av de ekonomiskt drivna grupperna går längre och har även kopplingar till statliga intressen. *APT41* med kinesisk anknytning kombinerar statssanktionerat spionage med cyberbrott för ekonomisk vinning. Genom avancerade tekniker och ett ständigt anpassningsbart arbetssätt kan de infektera hundratals system och försvåra spårning. På liknande vis bedriver den nordkoreanska *Lazarus Group* omfattande stölder och attacker, där intjänade medel stärker ett land under hårt ekonomiskt tryck. Dessa exempel visar hur gränsen mellan renodlade ekonomiska motiv och statliga strategier kan vara flytande.

Andra grupper saknar tydliga statliga kopplingar och drivs nästan uteslutande av ekonomiska incitament. *FIN7* (känd som Carbanak eller Navigator) riktar sofistikerade phishingattacker och skadlig kod mot banker, betalplattformar och andra ekonomiska institutioner, med stölder på över en miljard dollar. *Wizard Spider*, som verkar från Ryssland, använder spear-phishing och andra manipulativa metoder för att angripa stora företag, finansiella institutioner och till och med sjukvårdssektorn, där driftstopp och produktionsförluster ökar sannolikheten för att offren betalar lösensumman snabbt.

Dessa gruppers förmåga att ständigt ändra strategi och återuppstå i nya skepnader gör dem svåra att bekämpa. När denna rörlighet kombineras med RaaS-modellens enkla spridningsmöjligheter, växer utmaningarna med att stoppa ekonomiskt motiverad cyberkriminalitet.

Cyberattacker för politiska och sociala ändamål

Politiskt och Ideologiskt Motiverade Cyberattacker

I denna kategori återfinns grupper och aktörer som utnyttjar cyberangrepp för att främja specifika politiska, ideologiska eller sociala mål, snarare än enbart ekonomisk vinning.

Hacktivist-gruppen *Anonymous* är ett välkänt exempel. Denna löst sammansatta, decentraliserade rörelse genomför aktioner för att motverka övervakning och främja yttrandefrihet. Genom DDoS-attacker och intrång i känsliga system försöker de exponera maktmissbruk eller orättvisor hos regeringar och företag, med syftet att påverka den allmänna opinionen.

Liknande politiska drivkrafter kan ses hos *iranska* cyberaktörer som agerar under hacktivistisk täckmantel. Även om deras attacker ibland har ett ekonomiskt inslag, bygger de i hög grad på politisk motivation och geopolitiska intressen. Dessa aktörer riktar sig ofta mot kritisk infrastruktur och använder falska hacktivist-grupper för att dölja statliga operationer. Deras metoder har blivit alltmer sofistikerade och målinriktade, med internationella konsekvenser.

Ett annat exempel på aktörer med politiska kopplingar är *NSO Group*, ett israeliskt företag som utvecklar spionprogrammet Pegasus. Verktyget tros även ha sålts till statliga aktörer i syfte att övervaka journalister, politiska dissidenter och människorättsaktivister, vilket tydligt illustrerar hur cyberteknik kan användas för att både främja nationella intressen och förtrycka oppositionella röster.

Hackergruppen *Anonymous Sudan*, verksam under 2023, genomförde mer än 35 000 DDoS-attacker mot flera länder, däribland Sverige, Danmark, USA och Australien. Gruppen riktade in sig på kritiska sektorer som sjukhus, och det finns tecken på kopplingar till Ryssland. De har flitigt använt sitt varumärke och kommit med hot innan attacker för att skapa uppmärksamhet och sprida rädsla. Under 2024 stängde FBI, med stöd av Europol, ner Anonymous Sudan och inaktiverade deras kraftfulla DDoS-verktyg, vilket visar att även politiskt eller ideologiskt drivna grupper kan möta motstånd från internationella myndigheter.

Sammantaget visar dessa exempel hur cyberattacker för politiska och sociala ändamål inte bara handlar om att skada eller stjäla information, utan också om att påverka samhällen, forma opinion och stödja eller motverka nationella intressen.

”Teknik möjliggör automatisering, uppskalning och förbättrad precision, både på angriparsidan och försvarssidan,” *Kim Elman*.

Kim Elman *är en cybersäkerhetsexpert med en gedigen bakgrund inom underrättelse och säkerhet. Han har varit engagerad i att bygga upp Centrum för cybersäkerhet på forskningsinstitutet RISE. Dessutom är han grundaren av webbplatsen psykologisktforsvar.se som lanserades 2016. Elman har även arbetat på Vesper Group, ett företag som specialiserar sig på säkerhetslösningar och underrättelsetjänster. För närvarande är han Sverigechef på Northwave Cyber Security, ett företag som specialiserar sig på cybersäkerhet.*

AI-teknikens roll i framtidens angrepp och försvar

Elman beskriver hur AI-teknik och automatisering gör det möjligt att skapa processer som driver både attacker och försvar i stor skala med hög precision. Inom bedrägerier, där identiteter imiteras i text, bild eller video, används automatiserade metoder för att genomföra övertygande romansbedrägerier, vilket tydligt visar hur automatisering stärker kriminellas effektivitet.

Oheliga allianser och säkerhetsdilemman

Den geopolitiska situationen bidrar till en farlig växelverkan mellan stater och kriminella nätverk, där deras samarbete skapar vad Elman kallar "oheliga allianser". Ett exempel är Rysslands kopplingar till ransomware-grupper som utpressar ekonomiska måltavlor medan staten utnyttjar resultaten för spionage, sabotage och hybridangrepp.

Dessa allianser flätar samman kriminella och statliga intressen, där kriminella får ekonomisk vinning och stater strategiska fördelar inom teknik och geopolitik. För länder som Sverige skapar detta ett säkerhetsdilemma, där samordnade attacker mot företag och organisationer blir alltmer preciserade. Desinformation och hybridangrepp förstärker hotet och omformar det globala säkerhetslandskapet, vilket ökar behovet av innovativa försvarsstrategier.

Kriminell industrialisering

En framtida kriminell industrialisering kan innebära en alltmer specialiserad uppdelning av uppgifter inom brottsnätverk. Enligt Elman ser vi redan idag hur aktörer fokuserar på olika steg i kedjan: infiltrera en miljö, utnyttja system för att extrahera värdefull information och slutligen monetarisera och tvätta inkomsterna. Denna utveckling gör brottsligheten svårare att motverka.

Nya tekniska komponenter ger makt

Elman menar att beroendet av nuvarande och framtida teknologi diskuteras för lite. Sveriges beroende av Kina är särskilt stort inom grön teknik, både ekonomiskt och produktionsmässigt. Dessutom har vi ofta dålig insyn i vad de tekniska komponenterna faktiskt gör och hur de kommunicerar. Det finns en risk att dolda sårbarheter, som "trojanska hästar", kan finnas inbyggda i exempelvis laddboxar. Detta skulle kunna ge Kina ett betydande maktövertag, särskilt om en intressekonflikt skulle uppstå.

Data tar fram personporträtt - på vem som helst

En av de mer kontroversiella frågor som Elman tar upp är den psykografiska kartläggningen av individer. Han exemplifierar med Kinas strategiska informationsinsamling, där data om oss samlas in utan att vi kan vara säkra på hur den kommer att användas i framtiden. Genom denna kartläggning kan man med hög precision förutse hur någon kommer att rösta eller ha en viss åsikt. Detta är något som både kriminella aktörer och fientliga stater kan utnyttja.

Klimatet och arbetslöshetens påverkan

Elman tar även upp att klimatförändringar kan påverka försörjning och levnadsförhållanden. Migrationsströmmar och ökad sårbarhet kan utnyttjas av kriminella aktörer, exempelvis genom trafficking eller rekrytering till kriminella nätverk, vilket förvärrar exploatering och brottslighet.

Ett annat område Elman pekar på är AI:s påverkan på arbetsmarknaden. På kort sikt kan AI öka arbetslösheten, vilket kan tvinga vissa in i kriminalitet av desperation. På längre sikt förväntas dock samhället anpassa sig, skapa nya arbetstillfällen och därigenom minska risken för brottslighet.

Nya kriminella spelare omformar spelplanen

Kriminella nätverk och organiserad brottslighet har förändrats mycket de senaste åren. Det innebär nya utmaningar för både samhället och rättsväsendet. Här beskrivs nya aktörer som har identifierats i rapporten och som utmanar de tidigare strukturerna.

TEKNOLOGISKT AVANCERADE AKTÖRER

Den snabba digitala utvecklingen har skapat nya möjligheter för kriminella.

- Gränsöverskridande verksamhet: Brottslighet kan nu ledas, organiseras och bedrivas med delar av eller hela verksamheten utomlands.
- Krypterad kommunikation: Möjligheten att kommunicera i det fördolda via krypterade applikationer är ofta en förutsättning för moderna brottsupplägg.
- Cyberbrottslighet: Nya former av brott som utnyttjar digitala sårbarheter har uppstått.
- Dessa nya aktörer och metoder utmanar rättsväsendet och samhället genom att göra brottsligheten mer komplex, svårutredd och gränsöverskridande. Det kräver nya strategier och metoder för att effektivt förebygga och bekämpa denna typ av kriminalitet.

EKONOMISKA BROTTSLINGAR

Ekonomisk brottslighet har blivit en allt viktigare del av den organiserade brottsligheten.

- Återinvestering av brottsvinster: Stora summor återinvesteras i kriminell verksamhet, vilket ger aktörerna ännu större maktmedel.
- Välfärdsbrottslighet: Omfattande bedrägerier mot välfärdssystemen försvagar samhällets skyddsnät.
- Utnyttjande av finanssektorn: Nya möjligheter att flytta pengar, tvätta pengar och undandra skatt har uppstått.

UNGA KRIMINELLA

Allt yngre personer rekryteras till kriminella nätverk, ofta i åldrarna 12-15 år. Dessa rekryteras av något äldre ungdomar, vanligtvis 15-20 år gamla. Detta utmanar tidigare strukturer på flera sätt.

- Snabb rekrytering: Processen kan gå mycket fort, ibland på mindre än en dag.
- Generationsöverskridande: Den kriminella strukturen har byggts upp över generationer, vilket gör att olika åldersgrupper påverkar varandra.
- Svårare att motverka: Traditionella metoder för brottsbekämpning är ofta inte anpassade för så unga gärningsmän.

PROFESSIONALISERADE NARKOTIKA AKTÖRER

Narkotikamarknaden har genomgått en professionalisering som utmanar tidigare strukturer.

- Nya smugglingsmetoder: Mer sofistikerade och effektiva sätt att smuggla droger har utvecklats.
- Monopol på försäljningsplatser: Vissa aktörer har skaffat sig exklusiv kontroll över specifika områden.
- Ökad tillgänglighet: Nya distributionsmetoder har gjort det enklare för köpare att få tag på droger.

"Jag tror att vi som homosapiens har tappat kontrollen över den digitala världen vi lever i - men att vi kommer komma ifatt", *David Jacoby*.

David Jacoby *är en svensk IT-säkerhetsexpert och professionell etisk hackare med över 25 års erfarenhet inom området. Jacoby har blivit uppmärksammad som en av Sveriges främsta experter på digital säkerhet och har gjort sig ett namn internationellt för sina insikter och expertis. Han har också liknat sig själv vid karaktären Lisbeth Salander från Stieg Larssons Millennium-trilogi, vilket belyser hans djupa engagemang och skicklighet inom hackervärlden*

Digitaliseringen är fortfarande ung och bångstyrig

Jacoby reflekterar över hur ung vår digitala era är. Vi har stora förväntningar på att allt ska fungera smidigt, med lagstiftning, säkra produkter och tjänster. Men han menar att vi är naiva – vi förvånas över hur stora plattformar samlar enorma mängder data om oss. Med tiden, tror Jacoby, kommer vi att skapa struktur och säkrare system. Just nu lappas systemen ihop, men nya krav kommer driva utvecklingen framåt.

Många tycker att de inte har något av värde för hackare. Men när sociala mediekonton kapas inser man snabbt hur besvärligt det är – man tappar tillgång till bilder och nätverk. När den digitala hygienen inte sköts blir många människor smittade helt enkelt. Men det stora hotet uppstår när kriminella använder stulna profiler för att lura andra. Vår digitala profil blir ett verktyg för bedrägerier.

Jacoby anser att AI kommer förändra mänskligheten mer än internet. Han tror att många kognitiva funktioner kommer ersättas av digitala resurser och att AI kommer påverka hur vi tänker, kommunicerar och interagerar. Till och med våra känslor och begär kan snart tillgodoses genom virtuella miljöer.

Olika "valutor" driver brottslighet

Ett område som intresserar Jacoby är de olika "valutor" eller drivkrafter som kan motivera någon att begå brott. Fascinationen av att påverka något synligt, som att stoppa flygtrafik, kan vara lockande. Ilska och hämndbegär kan också fungera som en slags valuta för vissa. Idag ser vi att staters agerande, genom spektakel, kriser och att skapa osäkerhet, kan fungera som en form av valuta för att uppnå påverkan och manipulation.

Kriminella i ett enormt digitalt ekosystem

Jacoby lyfter fram hur digitaliseringen har skapat en global "arbetsplats" för kriminella. Numera kan de utföra attacker och intrång från vilken plats som helst i världen. Den digitala utvecklingen har också gjort det enkelt för kriminella att kommunicera internationellt och samarbeta genom att erbjuda specialiserade produkter och tjänster. Att skriva skadlig kod kräver inte längre egna tekniska kunskaper – det kan enkelt köpas av andra.

Jacoby belyser också den avancerade kompetens som vissa kriminella grupper eller individer besitter. I många fall har de utvecklat sina färdigheter genom högre utbildning, där samhället i praktiken har finansierat deras kunskap. Samtidigt består delar av denna kriminella värld av unga personer, ofta med erfarenheter från dataspelsvärlden. De drivs ibland av ilska eller en vilja att hämnas och kan lockas eller rekryteras av kriminella nätverk.

Dessa unga individer, som kanske inte ens förstår konsekvenserna av sina handlingar, arbetar i en digital miljö utan den sociala kontroll som präglar den fysiska världen. Detta bristande sociala skyddsnät gör det enklare för dem att glida in i brottslighet utan att känna rädsla för upptäckt.

Aktörer på spelplanen

Den kriminella spelplanen utgörs av aktörer med olika roller och funktioner – där det yttersta ledet är möjliggörare som verkar i näringslivet

Möjliggörare och specialister

Personer som har en möjliggörande roll för brottsligheten, till exempel professionella penningtvättare, jurister eller revisorer.

5%

Utförare - lägre skikt

Personer som genomför brottsliga handlingar på uppdrag, eller med stöd, av strategiska aktörer och utförare i högre skikt.

40%

Utförare - högre skikt

Personer som kan liknas vid platschefer som både utför delar av den brottsliga verksamheten, och tillser att den blir utförd.

38%

Strategiska/ledande aktörer

Personer som styr och leder den brottsliga verksamheten.

14%

Ur Polismyndighetens rapport ”Lägesbild över aktiva gängkriminella i Sverige 2024”

Möjliggörare och specialister

Personer som genomför brottsliga handlingar på uppdrag, eller med stöd, av strategiska aktörer och utförare i högre skikt.

5%

Hur fungerar möjliggörare inom kriminella nätverk?

Möjliggörare kan ha olika motiv för sina handlingar.

Vid ekonomiska motiv kan företagaren se en chans att öka faktureringen, eller den anställde att dryga ut lönen i utbyte mot att bidra till brottsliga upplägg.

Andra motiv kan vara känslomässiga, där en kriminell person spelar på kärlek eller lojalitet hos en myndighetsanställd som därigenom delar information eller utför tjänster.

Ett tredje motiv är kulturell gemenskap och grupptillhörighet, där starka band väger tyngre än lagen. En advokat, revisor eller mäklare kan välja att hjälpa en "bror" och därmed bortse från det lagliga ramverket.

Hur kan det komma att utvecklas framåt?

Internationellt sett finns trender som kan bidra till att antalet möjliggörare ökar.

Exempelvis kan illvilliga staters behov av spionage för att komma över företagshemligheter, som teknisk innovation, göra att möjliggörare inom företagen får en fortsatt viktig roll.

En annan trend är narkotikamarknadens omfattning, där de stora ekonomiska intäkterna från illegal narkotikahandel skapar ett behov av penningtvätt. Kriminella kan då komma att sätta upp ekonomiska strukturer som är kopplade till den legala sektorn, via företag och offentliga verksamheter, för att integrera sina olagliga intäkter.

Hur påverkas allmänheten?

När skatteflykt och förskingring av offentliga medel ökar, drabbas hela samhället. Resurser som skulle gå till välfärd och infrastruktur hamnar istället i kriminellas händer. Det leder till sämre levnadsvillkor, ökade samhällsklyftor och en minskad tillit till myndigheter.

Enligt Global Organized Crime Index 2023 är Sverige det land i Nordeuropa som är mest påverkat av organiserad brottslighet. Kriminella nätverk får allt starkare fäste, vilket hotar landets stabilitet och invånarnas trygghet.

Samtidigt visar EU-kommissionens prognoser för 2024 att Sveriges ekonomiska tillväxt är bland de lägsta i EU. Kombinationen av ökad brottslighet och en svag ekonomi skapar en komplex situation som hotar samhällsutvecklingen och medborgarnas framtidstro.

Utförare - lägre skikt

Personer som genomför brottsliga handlingar på uppdrag av, eller med stöd från, strategiska aktörer och utförare i högre skikt.

40%

Dålig skolgång, svaga band och statusbehov lockar unga till kriminalitet

Forskning visar att individer från lägre socioekonomiska grupper har en högre benägenhet att begå brott, vilket gör unga från utsatta områden särskilt sårbara för kriminalitet. En stabil skolgång fungerar som en viktig skyddsfaktor, medan unga som misslyckas i skolan eller hoppar av löper större risk att dras in i brottslighet.

Svag anknytning till familj, skola och samhälle, ökar risken för att unga begår brott. Samtidigt pågår en aktiv rekrytering inom gängkriminella miljöer, där allt yngre individer lockas att utföra kriminella handlingar. För många unga som söker status, respekt och tillhörighet kan kriminella grupperingar framstå som ett attraktivt alternativ, särskilt när föräldrakontrollen är svag och uppsikten över deras aktiviteter brister. Men även hållhakar kan tvinga unga att börja begå brottsliga handlingar.

Tidigt normbrytande beteende som inte uppmärksammas kan snabbt eskalera till allvarligare brott. För unga i ekonomiskt utsatta situationer blir även möjligheten till snabba pengar genom kriminalitet en stark lockelse.

Otrygghet och misstänksamhet skapar en negativ spiral

När allt yngre personer dras in i kriminalitet och allmänheten direkt påverkas, uppstår flera negativa konsekvenser. Känslan av otrygghet i samhället ökar, särskilt när brott begås i närmiljöer som bostadsområden, skolor och offentliga platser. Detta skapar en upplevelse av att ingen plats är säker, vilket kan leda till att människor blir mer misstänksamma och drar sig undan från att engagera sig i sina grannskap eller samhället i stort.

Den ökande brottsligheten innebär också ekonomiska konsekvenser, då kostnader för säkerhetsåtgärder och försäkringar stiger i takt med brott som inbrott, rån och skadegörelse. Även fastighetsvärden och näringslivet i drabbade områden kan påverkas negativt. För unga som dras in i kriminalitet finns en risk att hamna i en negativ spiral där misslyckanden i skolan leder till förlorade framtidsmöjligheter och en permanent koppling till en kriminell livsstil.

Denna utveckling belastar också rättssystemet och sociala tjänster, vilket påverkar samhällets resurser och möjligheten att hantera problemen på lång sikt.

Medelåldern i kriminella nätverk i Sverige är 28 år. Unga rekryteras in i en utförande roll där en tredjedel är under 18 år.

Utförare - högre skikt

Personer som kan liknas vid platschefer som både utför delar av den brottsliga verksamheten, och tillser att den blir utförd.

38%

Vilka exempel ser vi på detta?

Polisen uppskattar att antalet utförare i det högre skiktet – de så kallade platscheferna – är cirka 4800. Dessa personer befinner sig ofta på platser där de kan arbeta ostört, men ändå nära viktiga noder för internationell brottslighet, exempelvis i större städer eller mindre samhällen med kopplingar till gränshandel.

Platschefer har fler kontakter med andra aktiva inom kriminella nätverk än de utförare som finns i de lägre skikten. Två av tre platschefer har dessutom kontakter med kriminella i flera regioner utöver den egna. De kan även operera från länder med mindre strikt lagstiftning för att undvika rättsliga påföljder.

Som nyckelpersoner i nätverkens verksamhet är platschefer svåra att komma åt för rättsväsendet. De arbetar ofta med dolda och välorganiserade metoder, vilket gör det svårt att spåra och gripa dem.

Exempel på deras uppgifter

Strategisk planering: Utförare på denna nivå är ansvariga för att sätta upp och genomföra komplexa brottsplaner, från storskaliga bedrägerier till internationell smuggling och digitala brott.

Organisering och delegering: De samordnar aktiviteter mellan lägre nivåer av utförare och ser till att alla steg i operationen följs, från själva brottsliga handlingarna till hanteringen av resurser och pengar.

Uppdragshantering: Dessa aktörer driver ofta flera operationer samtidigt och koordinerar dem för att minimera risken för upptäckt.

Hur kan det komma att utvecklas framåt?

Utvecklingen framåt beror till stor del på hur effektivt rättsväsendet lyckas lagföra personer kopplade till kriminella nätverk. Om nyckelpersoner grips och strukturen försvagas kan det skapa ett maktvakuum som leder till interna konflikter, vilket i sin tur minskar nätverkets förmåga att utföra kriminella aktiviteter.

Samtidigt kan rättsväsendet få tillgång till viktig underrättelseinformation, vilket ger myndigheterna möjligheter att försvåra verksamheten ytterligare. Men om nätverket är starkt organiserat finns det risk att det återhämtar sig och fortsätter sin verksamhet trots motgångarna.

Strategiska/ledande aktörer

Personer som styr och leder den brottsliga verksamheten.

14%

Vilka exempel ser vi på detta?

De strategiska och ledande aktörerna i kriminella nätverk spelar en avgörande roll genom att styra och koordinera verksamheten utan att själva ofta delta i de direkta brottsliga handlingarna. Deras främsta uppgift är att planera, organisera och säkerställa att aktiviteter som narkotikahandel, vapenhandel och andra illegala transaktioner genomförs effektivt.

Ungefär 600 personer på topp- och mellannivå inom den kriminella hierarkin som opererar i Sverige är baserade utomlands, exempelvis i Spanien, på Balkan, samt i Mellanöstern, Nordafrika och Sydamerika. Deras syfte med att etablera sig utanför Sverige är dels att komma närmare den kriminella kärnverksamheten, som narkotikahandel, dels att undvika det svenska rättssystemet.

De fattar beslut om vilka brott nätverket ska fokusera på och utvecklar strategier för att undgå rättsväsendet. Detta innefattar att skapa logistiska planer för smuggling, penningtvätt och andra illegala aktiviteter. De kontrollerar nätverkets resurser – exempelvis pengar, droger och vapen – och ser till att dessa når de lägre nivåerna i organisationen som utför brotten. Genom kontakter i både kriminella kretsar och legitima företag underlättar de tillgången till resurser och möjliggör brott på hög nivå. Ofta sker detta med hjälp av insiders eller så kallade "möjliggörare".

Hur kan det komma att utvecklas framåt?

Framtiden för de strategiska och ledande aktörerna i kriminella nätverk kan ta olika riktningar, beroende på hur effektivt rättsväsendet agerar och hur skickliga de själva är på att undvika upptäckt. Om myndigheter utvecklar mer effektiva metoder för att lagföra dessa aktörer – till exempel genom ökad internationell samverkan och användning av avancerad teknik – kan deras roller försvåras. Detta skulle kunna leda till fragmentering av nätverken, där ledarna tvingas gömma sig eller förlorar sina positioner.

Ett effektivt sätt att bryta ner dessa nätverk långsiktigt är att störa deras ekonomiska flöden och affärsmodeller. Genom att rikta in sig på deras finansiering kan rättsväsendet minska deras förmåga att operera.

Om de kriminella ledarna däremot lyckas undvika upptäckt genom att gömma sig i andra länder och utnyttja digitaliseringens möjligheter, kan deras roller bli mer distansbaserade. Med hjälp av krypterade kommunikationer, mörka nätverk och illegala finansiella system kan de fortsätta att driva sina verksamheter på avstånd. Detta gör dem svårare att spåra och lagföra.

En sådan utveckling kan leda till att transnationella brottsnätverk växer sig ännu mer komplexa och resilienta, vilket ställer högre krav på internationell samverkan och innovativa metoder från rättsväsendet.

Branschanalys

Flera dynamiska krafter som nya aktörer, substitut och teknologisk innovation formar internationella brottsmarknaden

Den internationella brottsmarknaden är komplex och dynamisk, påverkad av flera krafter. För att förstå dessa krafter har vi använt Porter's Five Forces-modell, som analyserar hotet från nya aktörer, förhandlingsstyrkan hos köpare och leverantörer, konkurrensen mellan etablerade aktörer och hotet från substitutprodukter. Modellen ger en tydlig bild av de dynamiker som formar marknadens struktur och driver dess utveckling.

Analysen visar att hotet från nya aktörer är stort, vilket underlättar för nya grupper att etablera sig. Samtidigt tvingas etablerade aktörer anpassa sina strategier för att möta den ökade konkurrensen. Förhandlingsstyrkan hos leverantörer är hög i flera områden, särskilt där resurskontroll och specialisering spelar en avgörande roll. Köparnas förhandlingsstyrka är däremot begränsad, medan substitut, som nya brottsmetoder och teknologier, fortsätter att förändra marknaden och skapa nya utmaningar.

Hur påverkar olika marknadskrafter spelreglerna på den internationella brottsmarknaden?

Leverantörernas dominerande makt

Leverantörer, särskilt inom drog- och cyberbrottstjänster, har en stark ställning. Stora aktörer kontrollerar produktions- och distributionskedjan, vilket ger dem makt att påverka priser och villkor. Exempelvis kan stora narkotikakarteller diktera villkor för smugglare och mellanhandlare.

Intensiv konkurrens bland etablerade aktörer

Den kriminella marknaden är hårt konkurrensutsatt. Konflikter om territorier, marknadsandelar och distributionskanaler är vanliga, särskilt på narkotikamarknaden. Konkurrensen intensifieras ytterligare av priskrig, där aktörer försöker vinna mark genom lägre priser eller nya metoder.

Hotet från innovativa nya aktörer

Den internationella brottsmarknaden präglas av ett inflöde av nya aktörer. Dessa grupper använder ofta priskrig och nya teknologier för att ta sig in på marknaden, vilket tvingar etablerade aktörer att justera sina strategier. Krypterade kommunikationstjänster och dark web-plattformar gör inträdet enklare och sänker trösklarna för nya utmanare.

Hotet från nya substitut

Substitut spelar en växande roll inom den internationella brottsmarknaden. Nya former av brott, som cyberbrott med hjälp av open source-verktyg och avancerade teknologier, utmanar traditionella metoder och aktörer. Inom olika områden, som narkotikahandel och ekonomisk brottslighet, skapas alternativa produkter och tjänster som förändrar spelreglerna och påverkar både efterfrågan och lönsamhet för etablerade aktörer.

Köparnas begränsade förhandlingsstyrka

På grund av brottsmarknadens illegala natur är köparnas förhandlingsstyrka ofta svag. Leverantörerna har kontroll över både produktutbudet och distributionsvillkoren, medan köparna utsätts för stora risker i varje transaktion. Den fragmenterade köparbasen förstärker leverantörernas makt ytterligare.

Kriminell industrialisering

Precis som i övriga samhället har digitaliseringen möjliggjort nya tillvägagångssätt, bättre kommunikation, effektivitet och organisering.

Med nyttjandet av AI och annan ny teknik kan vi förvänta oss att denna utveckling inte bara fortsätter, utan accelererar och tillämpas i minst samma takt som i övriga samhället.

Kriminella aktörer utnyttjar samma innovationer som näringslivet

Automatisering av cyberbrott med AI

AI kan användas för att automatisera cyberattacker, vilket gör det möjligt för kriminella att genomföra fler och mer komplexa attacker med mindre ansträngning. Detta inkluderar phishing-attacker och ransomware, där AI bidrar till att identifiera sårbara mål och optimera attackerna.

Förbättrad dataintrångsteknik med AI

Med hjälp av AI kan kriminella analysera stora mängder data för att hitta säkerhetsbrister och genomföra dataintrång mer effektivt. AI kan användas för att förfalska autentiserings-uppgifter och kringgå säkerhetssystem. Zero Day-attacker, där säkerhetsproblem utnyttjas innan de upptäcks, är en särskilt avancerad metod som gör det svårt för organisationer att hinna åtgärda problemen.

Manipulation av information med deepfakes

Deepfakes gör det möjligt att skapa realistiska men falska bilder, videor och ljudklipp. Dessa kan användas för att sprida desinformation, utpressa individer och företag eller påverka offentliga opinioner. Dessutom kan deepfakes kringgå säkerhetssystem som ansikts- och röstigenkänning, vilket gör det enklare att få tillgång till skyddade system och ökar effektiviteten i cyberattacker.

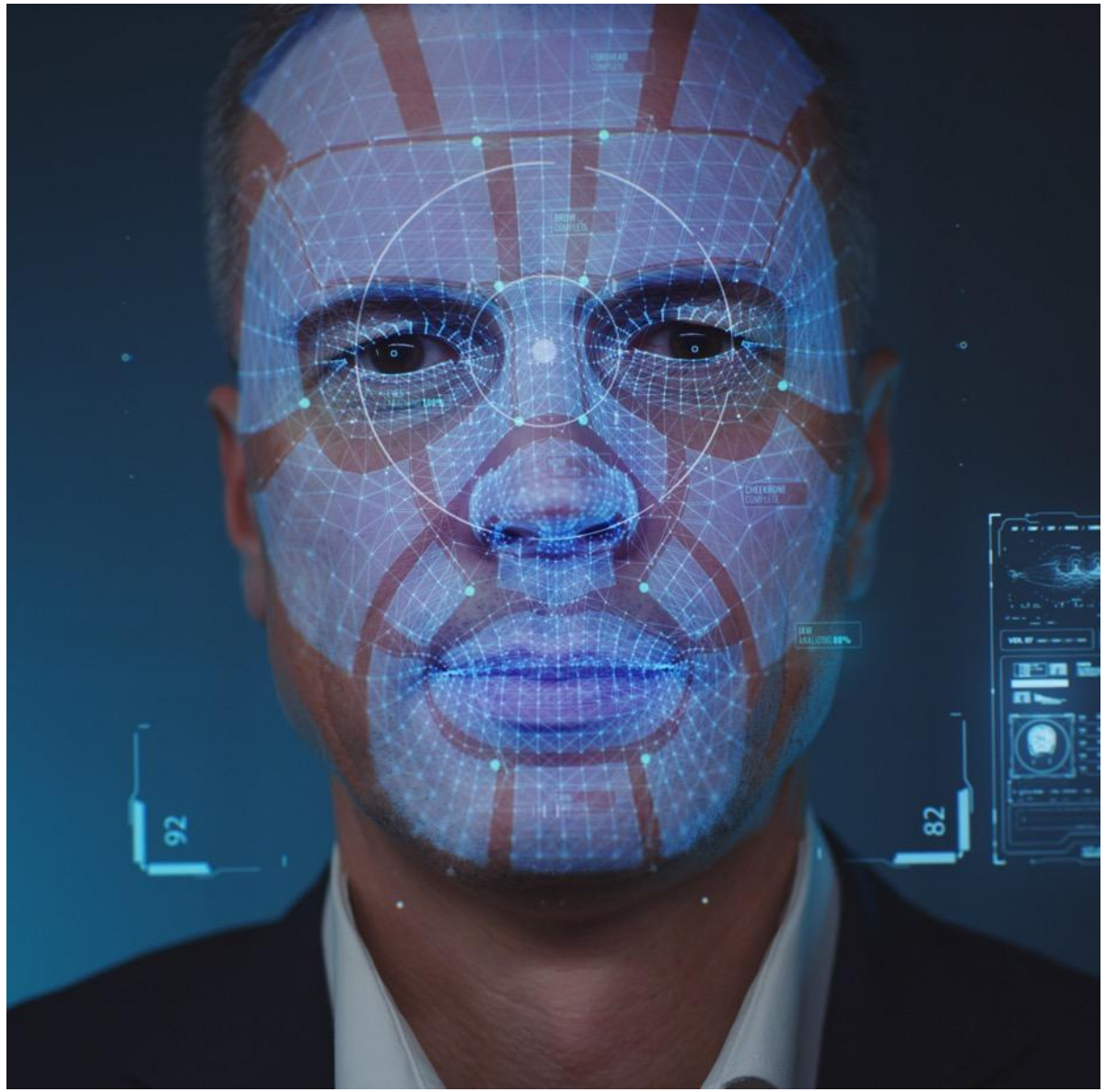
Penningtvätt och ekonomisk brottslighet med AI

Kriminella kan använda AI för att dölja ursprunget av olagligt erhållna pengar genom komplexa transaktioner och kryptovalutor. AI-algoritmer analyserar och manipulerar snabbt finansiella transaktioner för att undvika upptäckt och skapa avancerade metoder för penningtvätt.

AI-driven rekrytering och nätverksbyggande

AI möjliggör för kriminella att analysera sociala medieplattformar och online-nätverk för att identifiera och rekrytera nya medlemmar till sina nätverk. Genom dessa verktyg kan nätverken snabbt expandera och stärka sina organisationer på ett effektivt sätt.

Megatrender som påverkar



Megatrender som omformar framtidens spelplan och driver brottslighetens utveckling

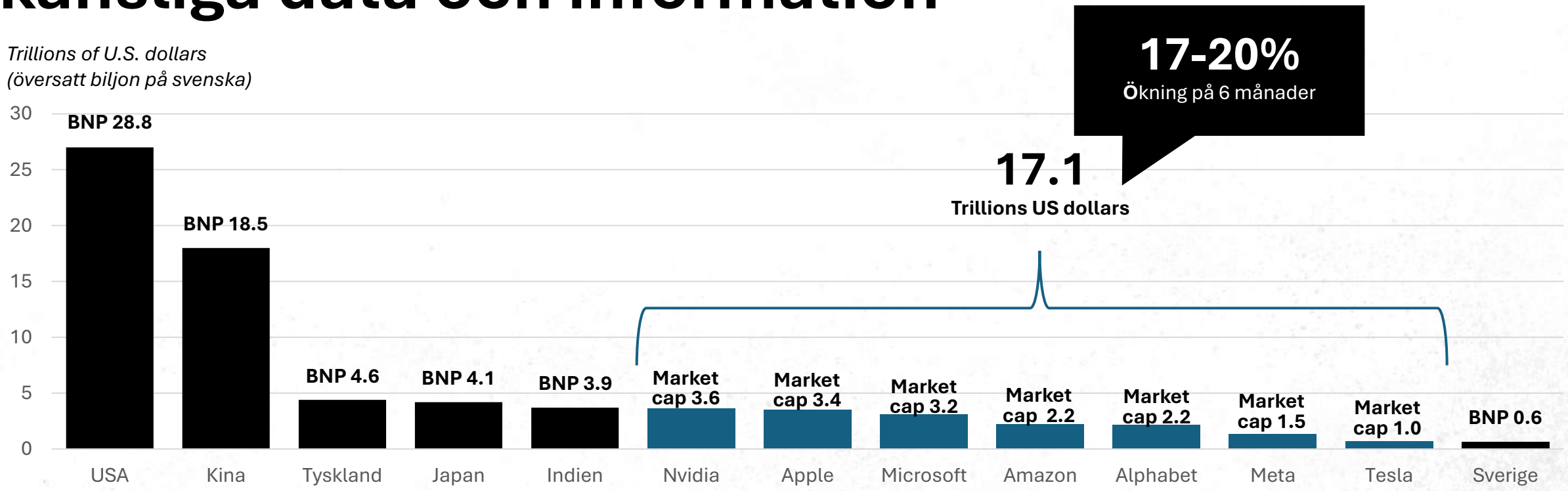
Brottsligheten genomgår en snabb och djupgående förändring, där teknologin fungerar som en kraftfull katalysator. Innovationer som artificiell intelligens, big data och automatisering skapar både möjligheter och risker – inte bara för samhällsutvecklingen, utan också för hur brottsliga aktiviteter utformas och utförs.

Techjättar har tagit en central roll som förvaltare av vår data, en roll som tidigare var förbehållen nationer och institutioner. Detta förändrar maktbalansen i grunden och skapar nya arenor för kriminalitet. Samtidigt ställer den så kallade AI-paradoxen oss inför akuta frågor: kan vi bevara demokratiska värden i en värld där deepfakes och hyperpersonaliserad manipulation blir vardagliga verktyg för påverkan?

Med teknikens snabba framsteg skapas också nya möjligheter för att utnyttja digitala fotspår och personlig information. Hyperdata – en avancerad form av datainsamling som kombinerar våra digitala beteenden, preferenser och svagheter – framträder som en resurs med enormt värde. Kriminella aktörer kan använda denna information på sätt vi ännu inte fullt ut kan förutse, vilket skapar nya sätt att utnyttja våra digitala liv och utmana våra skyddssystem.

Globala trender som klimatförändringar, ojämlikhet och digitalisering omformar förutsättningarna för brottslighetens utveckling. Dessa krafter skapar en ny spelplan där sociala, ekonomiska och teknologiska förändringar flätas samman. I detta avsnitt belyser vi hur dessa trender kan påverka framtidens brottslighet och de nya hot och möjligheter som växer fram i deras spår.

Techplattformarna växer sig större än de flesta nationer i världen – och det är de som sitter på vår allra mest känsliga data och information



Data hämtad 7 dec 2024

En framväxande **"teknopolär" ordning** – en där teknikföretag (AI) utövar den typ av makt inom sina domäner som en gång reserverades för nationalstater.

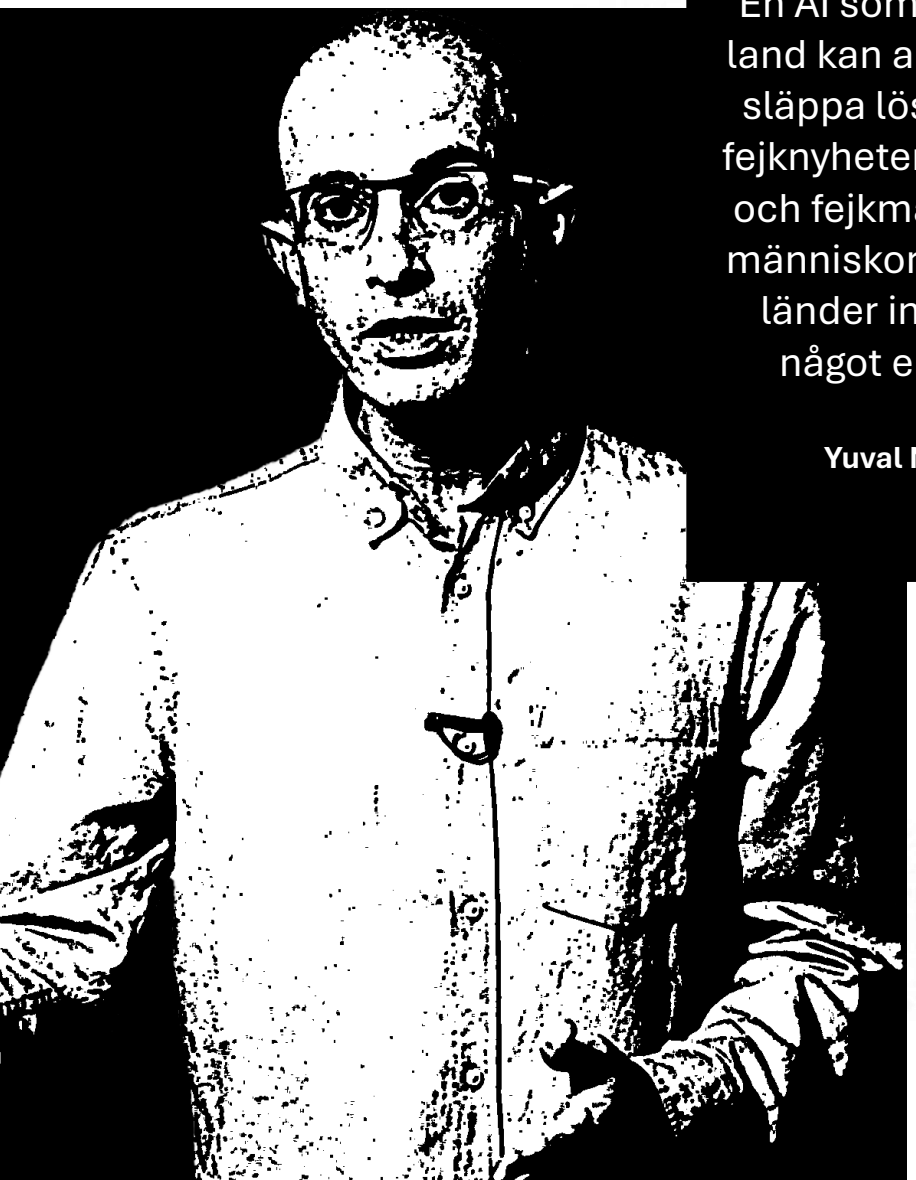
Ina Bremmer and Mustafa Suleyman

AI-kraftparadoxen: Möjligheter och risker i en AI-drivande värld

Snabbare, högre, starkare. AI erbjuder stora fördelar men medför också nya utmaningar som sätter mänsklig kontroll, förståelse och säkerhet på spel. Utmaningen ligger i att säkerställa att vi inte förlorar den mänskliga faktorn – kontrollen, förståelsen och ansvaret – i jakten på snabbare, högre och starkare tekniska lösningar.

"AI karakteriseras av 'dubbel användning'. Utveckling av generella system gör att AI i en applikation kan bota sjukdomar men också starta eller driva på sjukdomar. AI-utvecklingens decentraliserade karaktär och teknikens kärnegenskaper, såsom spridning av öppen källkod, ökar sannolikheten för att den kommer att beväpnas av cyberkriminella, statligt sponsrade aktörer och ensamma vargar.” – Ina Bremmer & Mustafa Suleyman

Denna paradox återspeglar också en framväxande "teknopolär" ordning, där teknikföretag – särskilt inom AI – börjar utöva en makt som tidigare reserverades för nationalstater. Tekniken är inte längre bara ett verktyg, utan en kraft som formar samhällsutvecklingen på djupgående sätt.



”En AI som utvecklats i ett land kan användas för att släppa lös en stormflod fejknyheter, falska pengar och fejkmänniskor så att människor i många andra länder inte kan lita på något eller någon”,

Yuval Noah Harari

”För första gången i mänsklighetens historia bygger vi ett samhälle med aliens,” Yuval Noah Harari.

Ur Dn:s artikel 240913 ” Yuval Noah Harari: ”AI ställer oss inför enorma existentiella kriser”.

AI hanterar lagar och ekonomi och blir på det sättet en del av samhället – utan att själva vara mänskliga. Demokrati är i grunden ett samtal mellan människor. Många gånger kaotiskt, fullt av röster i konflikt med varandra, men fortfarande ett samtal och mellan människor. Nu står vi inför ett oerhört stort dilemma – hur fungerar demokratin om några av de mäktigaste rösterna i det här samtalet inte längre är mänskliga?

Ökad ekonomisk ojämlikhet, fler naturkatastrofer, en förändrad arbetsmarknad och ny teknologi är exempel på megatrender som kan påverka den framtida brottsutvecklingen.

Globala trender som formar ett föränderligt landskap för brottsligheten

Teknologisk utveckling

Cyberattacker mer sofistikerade.

AI ökar hastigheten.

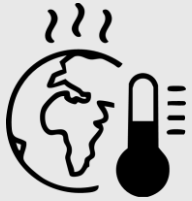
AI kraftparadoxen.

Samtidigt bidrar teknologi och digitalisering till förbättrad brottsprevention och polisarbete.

Ekonomisk ojämlikhet

Ojämlikhet inom och mellan länder kan skapa sociala spänningar och utanförskap.

Kan göra steget mot illegala ekonomier kortare. Särskilt samhällen med få legal alternativ till försörjning.



Klimat-förändringar

Naturkatastrofer.

Människor tvingas fly.

Steget till oönskade handlingar ökar för akuta behov av försörjning.

Risk för ökad människohandel.

Arbets-marknaden

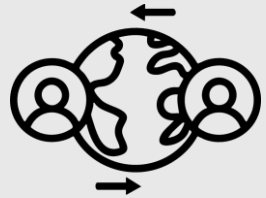
Hur ny teknologi påverkar arbetsmarknaden.

Hur den ekonomiska välfärden utvecklas.

Arbetslöshet.

Risk för ”extraknäck” för att dryga ut kassan.

Risk för exploatering av utsatta människor.



Globalisering av illegala marknader

Förenklar kriminella samarbeten mellan över nationsgränser.

Internet underlättar illegal handel, dark web och kryptovalutor.

Framtidens kriminella spelplan

Att analysera den kriminella spelplanen är en utmaning eftersom mycket av verksamheten sker i det fördolda, långt från insyn och transparens. Informationen är ofta bristfällig och svårbedömd, vilket komplicerar arbetet med att kartlägga och förstå denna dynamiska arena.

Trots dessa svårigheter har vi försökt identifiera och granska tendenser, innovationer och beteendemönster som kan prägla framtidens brottslighet. Genom vårt analysarbete har vi identifierat två särskilt framträdande utvecklingsspår – **"Den kriminella digitala evolutionen"** och **"Jakten på hyperpersonlig data"** – som tillsammans pekar mot hur den kriminella spelplanen kan förändras framöver.

”När avancerad teknik som AI, genetiska modifieringar och sammankopplade drönare blir mer tillgängliga ökar riskerna vid olämplig användning”, *Daniel Akenine*.

Daniel Akenine *är nationell teknikchef på Microsoft och en av Sveriges ledande experter inom digitalisering och framtidsteknologi. Med en bakgrund inom hjärnforskning och som medutvecklare av blockkedjeteknik kombinerar han teknisk expertis med djupa insikter i hur teknologi påverkar samhälle och kriminalitet. Han är också författare och har skrivit om teman som desinformation, artificiell intelligens och hur teknologins utveckling påverkar framtidens maktbalans.*

Kraftfull teknik blir både billigare och enklare att använda

När avancerad teknik som AI, genetiska modifieringar och sammankopplade drönare blir mer tillgängliga ökar riskerna vid olämplig användning. Det kommer troligen att krävas en striktare kontroll av denna typ av teknik i framtiden, inklusive möjligheten att förbjuda vissa typer av AI-användning. Den senaste AI-regleringen innehåller redan några sådana scenarier, men det är sannolikt att ytterligare användningsområden kan bli föremål för restriktioner när tekniken utvecklas och riskerna för negativa effekter ökar. Idag finns redan begränsningar kopplade till användning av biologisk krigsföring och kärnvapen, och samhället kan behöva dra lärdomar från dessa regleringar för att hantera ny teknologi på ett ansvarsfullt sätt.

Cyberbrott och statsstödda attacker blir allt vanligare

Ett annat område som Akenine lyfter fram är cyberbrott och statsstödda attacker. Dessa attacker, som oftast riktas mot att stjäla hemlig information, har blivit allt vanligare, med länder som Ryssland, Kina och Iran i spetsen. Han noterar att även om försvarare har en viss fördel eftersom de har mer kunskap om sina egna system, blir angriparna alltmer sofistikerade. Nationella statsattacker är ett växande bekymmer som Akenine menar måste tas på större allvar.

Dark Web, kriminalitet och övervakning

Akenine diskuterar också utmaningarna med dark web, där anonymitet bevaras med hjälp av teknologier som TOR-nätverket. Medan dessa teknologier kan ha legitima användningsområden, möjliggör de också kriminell verksamhet. Han betonar att även om dark web erbjuder en fristad för brott, använder många kriminella också den öppna webben då det är där de vanliga användarna och letande efter offer för bedrägerier sker.

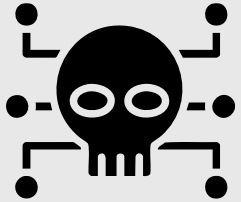
En av de mer kontroversiella frågor som Akenine tar upp är förslaget om CSAM-förordningen, ett lagförslag som skulle innebära att kommunikation inom Europa skannas för att upptäcka barnpornografi. Medan syftet är att förebygga fruktansvärda brott, finns en oro att denna infrastruktur skulle kunna användas för bredare övervakning i framtiden, vilket riskerar att urholka integriteten. Historiskt sett har Sverige varit en stark förespråkare för integritet, något som Akenine påpekar börjar förändras i takt med att samhället utsätts för ökande kriminalitet. Han beskriver hur integritet kan börja ses som en lyx som främst prioriteras när samhället inte står inför större problem. När allvarliga hot och risker uppstår, blir kompromisser med integriteten allt vanligare.

Kriminell infiltration

Slutligen diskuterar Akenine den ökande infiltrationen av kriminella i svenska myndigheter, särskilt i områden med hög gängkriminalitet. Han varnar för att Sveriges tidigare starka motståndskraft mot korruption håller på att försvagas, och att tecken på djupare infiltration har blivit allt tydligare.

Kriminalitetens digitala evolution:

Precis som i övriga samhället möjliggör AI och ny teknik nya tillvägagångssätt, bättre kommunikation och effektivitet



Automatisering av cyberbrott:

AI kan användas för att automatisera cyberattacker, vilket gör det möjligt för kriminella att genomföra fler och mer komplexa attacker med mindre ansträngning.

Detta inkluderar exempelvis phishing-attacker och ransomware, där AI kan hjälpa till att identifiera sårbara mål och optimera attackstrategier.

Förbättrad dataintrångsteknik:

AI hjälper kriminella att analysera data, identifiera säkerhetsbrister och genomföra intrång med precision. Det möjliggör även skapandet av falska autentiseringsuppgifter för att kringgå säkerhetssystem.

Zero Day-attacker utnyttjar sårbarheter okända för utvecklare, med noll tid att förbereda sig. Konsekvenserna kan bli omfattande för företag och kritisk infrastruktur.

Manipulation av information:

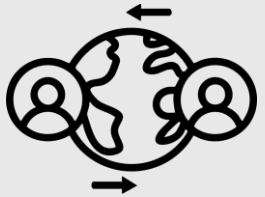
Deepfakes gör det möjligt att skapa realistiska men falska bilder, videor och ljudklipp som kan användas för att sprida desinformation, utpressa individer eller företag och påverka offentliga opinioner.

Det kan också öka effektiviteten av cyberattacker genom att kringgå säkerhetssystem som ansikts-eller röstigenkänning och göra det lättare att få tillgång till skyddade system.

Penningtvätt och ekonomisk brottslighet:

AI kan hjälpa kriminella att dölja ursprunget av olagligt erhållna pengar genom komplexa transaktioner och användning av kryptovalutor.

AI-algoritmer kan snabbt analysera och manipulera finansiella transaktioner för att undvika upptäckt.



Globalisering av illegala marknader:

AI kan användas för att analysera sociala medieplattformar och andra online-nätverk för att identifiera och rekrytera nya medlemmar till kriminella nätverk.

Detta gör det möjligt för kriminella att snabbt bygga och expandera sina nätverk.

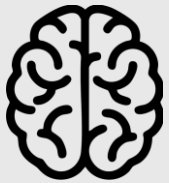
Under kommande 10 år kommer vi att se en ökning av en ny typ av brottslighet där nästa våg av digitalisering innebär en explosion av data och AI-tillämpningar. Nyttjandet av hyperpersonlig data står då på tur.

Vi kommer att se en kapprustning mellan säkerhetsexperter och cyberkriminella med en utveckling av allt mer avancerade attacker.

Jakten på hyperpersonlig data:

Hyperpersonlig data står i centrum för framtida brottslighet

Hyperpersonligt | **AI i avancerade upplägg**



Manipulation av hjärndata:

Med framsteg inom teknik som kan läsa av hjärnaktivitet finns risken att kriminella kan manipulera eller stjäla hjärndata för att påverka en persons tankar eller beteenden, vilket kan leda till nya former av bedrägeri eller utpressning.

Personligt dataintrång:

Enheter som samlar in detaljerad biologisk och psykologisk information kan bli mål för hackare som vill stjäla känslig personlig data. Denna data kan användas för identitetsstöld eller för att skapa skräddarsydda phishing-attacker.

Biometrisk datamissbruk:

Med ökad användning av biometriska data för säkerhetsändamål kan kriminella utnyttja AI för att skapa falska biometriska profiler, vilket kan användas för att kringgå säkerhetssystem och få obehörig tillgång till skyddade områden eller system.

Utveckling av giftiga ämnen:

AI kan användas för att analysera och designa kemiska strukturer, vilket kan leda till skapandet av nya giftiga ämnen. Detta kan utnyttjas av kriminella för att utveckla kemikalier som är svåra att upptäcka eller reglera.

Manipulering av forskningsdata:

AI kan användas för att manipulera forskningsdata och skapa falska resultat, vilket kan vilseleda forskningsinstitutioner och myndigheter kring säkerhet och effekter av vissa kemikalier eller biologiska agenter.

Avslutande reflektioner

Avslutande reflektioner

Sammanfattning av nyckelinsikter
I den här rapporten har vi försökt belysa de komplexa strukturer och dynamiker som präglar den kriminella spelplanen. Genom att undersöka kriminella grupper, deras organisering, aktörer och spelare samt brottstyper och branschanalys har vi fått en fördjupad bild och förståelse av deras anpassningsförmåga och strategiska utveckling. Från etablerade områden som narkotikahandel till framväxten av cyberbrott och framtida hyperpersonaliserade datautvinning, framgår det tydligt att dessa aktörer ständigt hittar nya sätt att utnyttja teknologiska och sociala trender.

Reflektion kring rapportens betydelse
Vi hoppas att insikterna i den här rapporten kan bidra till en bättre förståelse av kriminalitetens utveckling. Genom att identifiera trender och analysera de kriminella gruppernas strukturer och strategier kan vi på SSF, tillsammans med våra samarbetspartners, bidra till att utveckla mer effektiva brottsförebyggande åtgärder. Det är särskilt viktigt att uppmärksamma hur teknologin och globaliseringen både skapar nya möjligheter för legitima aktörer och samtidigt förstärker kriminalitetens potential att sprida sig och diversifieras.

Utmaningar och begränsningar
Under arbetets gång har vi mött flera utmaningar. En av de största har varit att få tillgång till tillförlitlig och uppdaterad information, särskilt inom snabbt föränderliga brottsområden som cyberbrott. Den kriminella verksamheten sker ofta i det dolda, vilket innebär att insynen i deras operationer är begränsad. Dessutom är områdets komplexitet en utmaning i sig, där relationer mellan olika aktörer och grupper inte alltid är tydliga eller bestående.

Framtida frågor
Vi ser flera områden som skulle vara värda att utforska vidare. En djupare analys av hur ny teknologi som AI och kvantdatorer kan användas av kriminella aktörer är särskilt angelägen. Vi är också nyfikna på att undersöka hur vårt allt mer uppkopplade vardagsliv kan utnyttjas av kriminella för att eskalera hot och attacker mot smarta städer och smarta hem. Vidare vill vi följa och försöka förstå hur den kriminella spelplanen påverkas av globala händelser, som ekonomiska kriser och geopolitiska spänningar. Ett annat viktigt område är att närmare granska sociala och ekonomiska faktorer som kan bidra till att nya individer rekryteras in i kriminalitet.

Avslutande tanke
Kriminalitetens roll i samhället är under ständig utveckling, och det kriminella landskapet är en spelplan där aktörer och strategier ständigt förändras. Samtidigt som teknologiska framsteg skapar nya möjligheter för legitima aktörer ser vi också en växande utmaning för samhället att bekämpa kriminalitet. Vi hoppas att den här rapporten kan vara ett bidrag till att analysera, förstå och agera för att skydda vårt samhälle från de hot som ständigt skiftar och utvecklas. Vi ser fram emot fortsatt dialog och kunskapsutbyte med andra som verkar inom detta viktiga område.

Framtidens Brott är en rapportserie på initiativ av SSF

Rapporten ”Den Kriminella Spelplanen” är en utgåva i SSF koncept Framtidens Brott som tagits fram 2024. En andra rapport publiceras våren 2025 och en tredje och fjärde rapport utkommer senare på året.

Expertintervjuer:

Daniel Akenine
Nationell teknikchef på Microsoft Sverige

Kim Elman
Sverigechef Northwave, tidigare Centrum för cybersäkerhet på forskningsinstitutet RISE

David Jacoby
Etisk hackare och IT-säkerhetsexpert

Evin Cetin
Jurist, författare och samhällsdebattör

Joakim Kävrestad
Akademiker och expert inom informationsteknologi vid Tekniska Högskolan i Jönköping

John Forsberg
Chef för utvecklingscentrum Nord, Nationella operativa avdelningen (NOA) inom Polismyndigheten

Projektgrupp:

Ulrika Hallesius
Kriminolog på SSF Stöldskyddsföreningen
ulrika.hallesius@stoldskyddsforeningen.se

Charlotte Mattfolk
Framtidsanalytiker på IAMAI

Definitioner av organiserad brottslighet och kriminella nätverk

Organiserad brottslighet
FN definierar organiserad brottslighet utifrån begreppet ”organiserad kriminell grupp”. Vilket definieras genom fyra kriterier: brottslighet som en grupp bestående av tre eller fler personer, som under en längre tid agerar i samförstånd, med syftet att begå minst ett grovt brott, för ekonomisk eller materiell vinning.

EU definierar organiserad brottslighet genom kriterier där minst sex måste uppfyllas, varav fyra är obligatoriska: samarbete mellan fler än två personer, lång varaktighet, misstanke om allvarliga brott och strävan efter vinning eller makt. Andra kännetecken kan vara tilldelade uppgifter, disciplin och kontroll, lokal verksamhet, användning av våld, penningtvätt eller otillbörlig påverkan på politik, medier och ekonomi.

Den svenska Polismyndigheten definierar organiserad brottslighet som en verksamhet där minst två personer samarbetar över tid för att begå allvarliga brott i syfte att uppnå ekonomisk vinning. Denna definition används inom den myndighetsgemensamma satsningen mot organiserad brottslighet och betonar samarbete, varaktighet, allvarlig brottslighet och ekonomiskt motiv.

Kriminella nätverk
Enligt Polismyndigheten finns det inte någon definition av begreppet ”kriminella nätverk” i svensk rätt. Begrepp som ”gängkriminalitet”, ”organiserad brottslighet”, ”kriminella miljöer” och ”kriminella nätverk” används ofta synonymt för att beskriva brottslighet som innebär någon form av samverkan inom en struktur. Avsaknaden av en definition av ”kriminella nätverk” innebär att bedömningar av antalet personer i de kriminella miljöerna varierar beroende på sammanhang, och på hur underlag sammanställs.

Det finns olika typer av kriminella nätverk, exempelvis mc-gäng, familje- och släktbaserade nätverk, samt stadsdels- och förortsbaserade grupper. Dessa nätverk skiljer sig åt i graden av organisation, hierarkiska strukturer och antal medlemmar. De kan vara både bestående över tid eller tillfälliga i sin form.

Dessa nätverk kan variera i organisationsgrad, hierarki och antal individer, och de kan vara både beständiga över tid eller tillfälliga. De omfattar allt från hierarkiska och formaliserade organisationer till lösare grupperingar.

Angränsande begrepp som ”gängkriminalitet”, ”organiserad brottslighet”, ”kriminella miljöer” och ”kriminella nätverk” används ofta synonymt för att beskriva brottslighet som bygger på någon form av samverkan inom en struktur.

Maffia

En organiserad internationell brottsorganisation som ursprungligen opererade på Sicilien och nu särskilt i Italien och USA, och som har en komplex och hänsynslös beteendekod utvecklad under 1700- och 1800-talen. Ordet kommer från italienska (siciliansk dialekt), ursprungligen i betydelsen 'skrytsamhet’.

Enskilda kriminella
Trots den omfattande organiserade brottsligheten begår många individer fortfarande brott på egen hand. Dessa enskilda kriminella agerar ofta mer sporadiskt och utan samma grad av organisering. Exempel på brott som begås av individer inkluderar stöld och inbrott, ekonomiska bedrägerier, skattebrott, våldsbrott samt narkotikabrott.

Källor

I arbetet med rapporten har vi samlat kunskap om kriminell organisering och ekonomi från myndighetsrapporter (Polismyndigheten, Brå, Ekobrottsmyndigheten, Europol, Interpol med flera), analyser från det privata näringslivet, journalistiska granskningar samt internationella experter och forskare inom områden som AI, politik och samhällsvetenskap. Referenser finns per sida och som länkar för dig som vill fördjupa dig ytterligare i ämnet.

Sidor med källhänvisningar:

7: Digitaliseringen skiftar vardagsbrottslighetens fokus
Brå *https://bra.se/statistik/kriminalstatistik.html*
Bilbrottsbarometern *https://via.tt.se/files/391729/3440144/62595/sv*
8: Den kriminella ekonomin
Polismyndigheten https://polisen.se/om-polisen/polisens-arbete/kriminell-ekonomi/
Polismyndigheten https://polisen.se/aktuellt/nyheter/stockholm/2024/september/kriminell-ekonomi-beskrivs-i-ny-rapport-fran-region-stockholm/
Nasdaq https://www.nasdaq.com/global-financial-crime-report
https://www.occrp.org/en/news/global-financial-crime-report-criminals-took-us31-trillion-in-2023
9: Den kriminella världen
Polismyndigheten https://polisen.se/aktuellt/nyheter/nationell/2024/februari/totalt-62-000-bedoms-aktiva-eller-ha-koppling-till-kriminella-natverk/
Brå *https://bra.se/publikationer/arkiv/publikationer/2023-11-01-barn-och-unga-i-kriminella-natverk.html*
Bohuslänningen *https://www.bohuslaningen.se/asikt/ledare/brottsligheten-har-gatt-fran-lokal-till-global.003eeb4f-c190-4ade-bb51-0def0f274351*
SVT https://www.svt.se/nyheter/inrikes/600-gangkriminella-utomlands-styr-brottsligheten-i-sverige
Europol https://www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks
SVT *https://www.svt.se/nyheter/utrikes/europol-har-kartlagt-de-821-farligaste-kriminella-natverken-i-Europa*
10: Nätpatrullering
Europol https://www.europol.europa.eu/media-press/newsroom/news/cyber-blue-line-%E2%80%93-new-law-enforcement-frontier
SVT https://www.svt.se/nyheter/lokalt/vasterbotten/umeapolisen-john-ska-patrullera-pa-natet
12: Kriminella nätverk använder vanliga företag som täckmantel
Ekobrottsmyndigheten https://www.ekobrottsmyndigheten.se/kriminella-foretag-utnyttjar-de-svenska-valfardssystemen/
SVT *Europol har kartlagt de 821 farligaste kriminella nätverken i Europa | SVT Nyheter*
Stockholms Handelskammare https://stockholmshandelskammare.se/nyheter/ny-rapport-visar-kopplingarna-mellan-naringslivet-och-den-organiserade-brottsligheten/?utm_source=chatgpt.com
13. Nasdaq
Linkedin *https://www.linkedin.com/posts/adenatfriedman_financial-crime-is-an-invasive-drag-on-our-activity-7240054480640126976-pPO4*
OCCRP https://www.occrp.org/en/news/global-financial-crime-report-criminals-took-us31-trillion-in-2023
14: Kriminella organisationer smälter in i samhället
YLE *https://svenska.yle.fi/a/7-1511137*
SVT *https://www.svt.se/nyheter/inrikes/uppgifter-dad-mot-ambassader-i-stockholm-och-kopenhamn-ska-ha-utforts-pa-uppdrag-av-foxtrot*
Dagens PS https://www.dagensps.se/foretag/kriminella-tar-over-i-svenskt-naringsliv-riskerar-bli-som-italien

Fortsättning källor

Sidor med källhänvisningar:

15. Den svarta svanen
TV2 DK *https://play.tv2.dk/serie/den-sorte-svane-tv2*
SVT https://www.svtplay.se/den-svarta-svanen
Ekobrottsmyndigheten https://www.ekobrottsmyndigheten.se/kriminella-foretag-utnyttjar-de-svenska-valfardssystemen/
Publikt https://www.publikt.se/fordjupning/pa-djupet/statens-anstallda-blir-verktyg-kriminella-25257
17: Internationella kriminella nätverk påverkar vanliga medborgares livsstil
Ekobrottsmyndigheten https://www.ekobrottsmyndigheten.se/om-ekobrott/
Regeringen https://www.regeringen.se/contentassets/1ae2655654ab479d8e4210d12f44e816/motstandskraft-och-handlingskraft---en-nationell-strategi-mot-organiserad-brottslighet-skr.-20232467
Internetstiftelsen https://svenskarnaochinternet.se/rapporter/svenskarna-och-internet-2021/nathat-och-natbrott/
Polismyndigheten *https://polisen.se/siteassets/dokument/ovriga_rapporter/en-nationell-oversikt-av-kriminella-natverk.pdf/download/*
LO https://lo.se/start/tal_och_artiklar/svartjobb_innebar_stora_risker_for_bade_individer_och_samhalle
18: Internationella kriminella nätverk påverkar företag i Sverige på flera sätt
Företagarna https://www.foretagarna.se/politik-paverkan/rapporter/2022/brott-mot-foretagare/
LO https://lo.se/start/tal_och_artiklar/svartjobb_innebar_stora_risker_for_bade_individer_och_samhalle
Almega https://www.almega.se/2024/07/ny-rapport-dold-brottslighet-sa-drabbas-tjanstesektorn-av-den-radande-brottsligheten/
Stockholms handelskammare https://stockholmshandelskammare.se/rapporter/rapport-kriminella-entreprenorer-en-studie-av-den-organiserade-brottslighetens-kopplingar-till-naringslivet/
Dagens PS *Företagare: "Kriminella hindrar oss" - Dagens PS*
21-22. The Old Big Crim
Europol *https://www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks*
Interpol https://www.interpol.int/en/Crimes/Organized-crime/INTERPOL-Cooperation-Against-Ndrangheta-I-CAN
SR https://sverigesradio.se/avsnitt/sa-kan-kinesiska-maffians-brutala-metoder-komma-till-sverige
Insight Crime https://insightcrime.org/news/analysis/the-business-relationship-between-italys-mafia-and-mexicos-drug-cartels/
SRF https://www.srf.ch/news/international/mafia-prozess-in-kalabrien-die-ndrangheta-und-ihre-gehilfen-auf-der-anklagebank
The Times UK https://www.thetimes.co.uk/article/making-a-mafia-how-a-brutal-kidnapping-honed-the-ndrangheta-62tkqbskr
Wikipedia https://sv.wikipedia.org/wiki/Yakuza
YLE https://yle.fi/a/7-1375504
CEPR Center for economic policy research https://cepr.org/voxeu/columns/boss-board-mafia-infiltrations-firm-performance-and-local-economic-growth
The Times World https://www.thetimes.com/world/latin-america/article/narco-submarines-8-billion-pacific-drug-bust-97jljmp2h
Wikipedia https://sv.wikipedia.org/wiki/Ryska_maffian

Fortsättning källor

Sidor med källhänvisningar:

23-27: The New Big Crim
IOCTA https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf
MSB https://www.msb.se/contentassets/fe72c449466e4017bd76787762ab9dc5/rapport-cybersakerhet-i-sverige-2020--hot-metoder-brister-och-beroenden.pdf
Europol https://www.europol.europa.eu/publication-events/main-reports/decoding-eus-most-threatening-criminal-networks
Europol https://www.europol.europa.eu/cms/sites/default/files/documents/SV_Decoding%20Report%20%E2%80%94%20Sammanfattning.pdf
Microsoft https://learn.microsoft.com/en-us/defender-xdr/microsoft-threat-actor-naming
Nordvpn https://nordvpn.com/cybersecurity/glossary/adversary-group-naming/
https://essay.utwente.nl/101586/1/Hasper_MA_BMS.pdf
https://pstirparo.ch/posts/threat-actor-naming-taxonomies/
The Hacker news https://thehackernews.com/2024/04/fin7-cybercrime-group-targeting-us-auto.html
Crowd Strike https://www.crowdstrike.com/en-us/blog/big-game-hunting-with-ryuk-another-lucrative-targeted-ransomware/
Crowd Strike https://www.crowdstrike.com/en-us/blog/wizard-spider-adversary-update/?utm_source=chatgpt.com
Industrial Cyber https://industrialcyber.co/reports/prodaft-report-throws-light-on-financially-motivated-wizard-spider-cybercrime-group/
Cloudflare https://www.cloudflare.com/learning/ddos/glossary/anonymous-sudan/
Europol https://www.europol.europa.eu/media-press/newsroom/news/charges-unveiled-in-ongoing-effort-to-de-anonymise-ddos-group-anonymous-sudan-0
29: Nya kriminella spelare omformar spelplanen
Riksdagen https://www.riksdagen.se/sv/dokument-och-lagar/dokument/skrivelse/motstandskraft-och-handlingskraft-en-nationell_hb0367/html/
Regeringen https://www.regeringen.se/contentassets/f1f723f5055742ada170f2ae758a0c5f/ett-fortydligat-brottsforebyggande-ansvar-for-socialnamnden.pdf
Brå https://bra.se/forskning-och-analys/organiserad-brottslighet.html
Brå https://bra.se/amnen/barn-och-ungas-brottslighet
32-36: Den kriminella spelplanen utgörs av aktörer med olika roller och funktioner
Polismyndigheten https://polisen.se/siteassets/dokument/regeringsuppdrag/lagesbild-over-aktiva-gangkriminella-i-sverige-.pdf
Polismyndigheten *https://polisen.se/aktuellt/nyheter/nationell/2024/februari/totalt-62-000-bedoms-aktiva-eller-ha-koppling-till-kriminella-natverk/*
Global organized crime index https://ocindex.net
Forum https://www.forum.se/nyheter/maffiapakten-nar-samhallets-betrodda-saljer-sig-till-gangen/
Global organized crime index *https://ocindex.net*
Publikt *https://www.publikt.se/fordjupning/pa-djupet/statens-anstallda-blir-verktyg-kriminella-25257*
Lasse Wierup https://www.forum.se/bocker/267302/gangsterparadiset/
Polismyndigheten https://polisen.se/aktuellt/nyheter/nationell/2024/oktober/sa-kan-den-digitala-rekryteringen-av-barn-och-unga-till-kriminalitet-ga-till/
Socialstyrelsen https://www.socialstyrelsen.se/kunskapsstod-och-regler/omraden/barn-och-unga/unga-som-begar-brott/
Brå *https://bra.se/amnen/barn-och-ungas-brottslighet*
Brå *https://bra.se/forebygga-brott/forebyggande-utifran-amne/barn-unga-och-brott.html*
Brå *https://bra.se/publikationer/arkiv/publikationer/2024-03-01-mojliggorare-for-kriminella-natverk.html*
SVT Nyheter https://www.svt.se/nyheter/inrikes/600-gangkriminella-utomlands-styr-brottsligheten-i-sverige

Fortsättning källor

Här följer de sidor som har källhänvisningar:

39: Branschanalys - Fler dynamiska krafter som nya aktörer, substitut och teknologisk innovation
Europol https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf
United Nations https://www.unodc.org/documents/data-and-analysis/WDR_2024/WDR_2024_SPI.pdf
SVT https://www.svt.se/nyheter/sapmi/drogkartellerna-tranger-undan-urfolken-ser-att-valdet-okar
Atlantic Council https://www.atlanticcouncil.org/in-depth-research-reports/issue-brief/behind-the-rise-of-ransomware/
40: Kriminell industrialisering
Europol *https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf*
PWC *https://www.pwc.com/m1/en/publications/documents/2024/the-future-of-crime-eng.pdf*
43: Techplattformar
IMF https://www.imf.org/external/datamapper/NGDPD@WEO/OEMDC/ADVEC/WEOWORLD
Statista https://www.statista.com/statistics/1350976/leading-tech-companies-worldwide-by-market-cap/
44: AI-kraftparadoxen
Ted https://www.ted.com/talks/mustafa_suleyman_what_is_an_ai_anyway?subtitle=en
Foreign Affairs https://www.foreignaffairs.com/world/artificial-intelligence-power-paradox
45: För första gången i mänsklighetens...
DN https://www.dn.se/kultur/yuval-noah-harari-ai-staller-oss-infor-enorma-existentiella-kriser/
https://www.ynharari.com/
https://www.ynharari.com/book/nexus/?_gl=1*lzwkvz*_up*MQ..*_ga*MjAwNDg5NTQ2NS4xNzM0Njg2NDc5*_ga_3VXWK7L4ZR*MTczNDY4NjQ3OC4xLjAuMTczNDY4NjQ3OC4wLjAuMA..
46: Globala trender som formar ett föränderligt landskap för brottsligheten
Utrikespolitiska institutionen *https://www.ui.se/utrikesmagasinet/analyser/2021/juni/pandemin-skjuter-ner-de-globala-utvecklingsmalen/*
FN *https://unric.org/sv/fn-rapport-att-hantera-ojamlikhet-ar-svaret-pa-de-globala-protester-vi-ser/*
Akademikern *https://akademikern.se/ny-rapport-okande-ojamlikhet-medfor-risker-for-hela-samhallet/*
Verkliga Brott *https://verkligabrott.se/inverkan-av-socioekonomiska-faktorer-pa-brottslighet-i-sverige/*
FN *https://www.undp.org/sv/sweden/press-releases/11-miljarder-manniskor-lever-i-flerdimensionell-fattigdom-och-nastan-en-halv-miljard-av-dem-lever-i-konfliktomraden*
Södertörns Högskola *https://www.sh.se/nyheter/forskning/2024-01-11-hur-paverkar-inflation-och-arbetsloshet-brottsligheten-ny-forskning-soker-svaret*
Nordiska ministerrådet *https://pub.norden.org/nord2024-005/summering-och-nyckelbudskap-om-ekonomisk-utsatthet-i-norden.html*
Oxfam *https://policy-practice.oxfam.org/resources/global-megatrends-mapping-the-forces-that-affect-us-all-620942/*
Future Policing Institute *https://www.futurepolicing.org/future-concepts/blog-post-title-one-bek8y-2rbw2-atkk3*
49-50: Kriminalitetens digitala evolution och Jakten på hyperpersonlig data
PWC *https://www.pwc.com/m1/en/publications/documents/2024/the-future-of-crime-eng.pdf*
CGI https://www.cgi.com/sites/default/files/2022-09/cgi-nl_whitepaper_data-security-risks-cyber-resilience-hyperconnected-world.pdf
AXA XL Insurance *https://axaxl.com/fast-fast-forward/articles/deepfakes_an-emerging-cyber-threat-that-combines-ai-realism-and-social-engineering*
Cointelegraph *https://cointelegraph.com/news/ai-deepfake-scams-threaten-crypto-wallets-2024*
Europol IOCTA https://www.europol.europa.eu/cms/sites/default/files/documents/Internet%20Organised%20Crime%20Threat%20Assessment%20IOCTA%202024.pdf
CEPA https://cepa.org/article/data-as-ammunition-hyper-personalized-warfare-in-the-digital-age/
Lexology https://www.lexology.com/library/detail.aspx?g=93ff642e-0026-4f99-ba79-0fae4114ded5
54: Definitioner
Oxford reference https://www.oxfordreference.com/display/10.1093/oi/authority.20110803100125354
Europol https://www.europol.europa.eu/socta/2017/defining-serious-and-organised-crime.html
Polismyndigheten https://polisen.se/siteassets/dokument/regeringsuppdrag/lagesbild-over-aktiva-gangkriminella-i-sverige-.pdf/download/?v=f8edd8d100b188a6937b44efc91a30ea
Polismyndigheten https://polisen.se/om-polisen/polisens-arbete/organiserad-brottslighet/
Polismyndigheten https://polisen.se/om-polisen/polisens-arbete/organiserad-brottslighet/myndighetsgemensam-satsning-mot-organiserad-brottslighet/